PARLIAMENT
Bridgetown, Barbados

REPORT

OF THE

JOINT SELECT COMMITTEE (STANDING)

ON

GOVERNANCE AND POLICY MATTERS

ON THE

CYBERCRIME BILL, 2024

AND THE

MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024

REPORT

OF THE

JOINT SELECT COMMITTEE (STANDING)

ON

GOVERNANCE AND POLICY MATTERS

ON THE

CYBERCRIME BILL, 2024

AND THE

MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024

1. The Honourable the Senate on 14th February, 2024 committed, with the concurrence of the Honourable the House of Assembly on the 16th February, 2024, the following Bills:

Cybercrime Bill, 2024 and the **Mutual Assistance in Criminal Matters (Amendment) Bill, 2024**

to the Joint Select Committee (Standing) of the two Houses of Parliament **(hereafter referred to as "the Committee")** comprising four (4) members of the Honourable the House of Assembly and three (3) members of the Honourable the Senate.

2. The Committee's membership is as follows:

Mr. Edmund G. Hinkson, S.C., M.P. *(Chairman)*
Mr. Peter R. Phillips, J.P., M.P.
Dr. Romel O. Springer, J.P., M.P. *(Deputy Chairman)*
Mr. Ralph A. Thorne, K.C., M.P.
Senator Gregory P. B. Nicholls
Senator Ryan O. Walters
Senator the Hon. Lindell E. Nurse

3. The Committee approved the following terms of reference:

TERMS OF REFERENCE

1. To enquire into and determine whether the Cybercrime Bill as drafted fulfils the expressed purposes to ensure compliance with the International Conventions, global standards and best practices to counter cybercrime and to ensure international cooperation in the combatting of cybercrime.

2. To examine whether the Cybercrime Bill as drafted curtails the citizens' fundamental rights to freedom of expression as against the protection of the reputation, rights and freedoms of other persons or their private lives.

3. To examine whether the Cybercrime Bill as drafted provides the necessary checks and balances, safeguards and independent oversight to protect citizens' human rights, liberties and privacy rights from potential abuses, including from expansive law enforcement powers in order to prevent miscarriages of justice.

4. To examine whether the Cybercrime Bill as drafted provides adequate protection to all of the specific categories of persons who may potentially be vulnerable to cybercrime.

5. To examine whether any of the provisions of the Cybercrime Bill as drafted are vague, overly broad, arbitrary and/or subjective and uncertain in its imposition of liability.

6. To examine whether the penalties imposed in the Cybercrime Bill as drafted are disproportionate and/or unreasonable in any way.

7. To examine whether the Cybercrime Bill as drafted provides adequate protection for whistleblowers who expose cyber-related wrongdoing and, if not, whether such protection is provided in any other legislation.

8. To consider whether the Cybercrime Bill as drafted could impede innovation in the technology sector and discourage investment and research in digital infrastructure.

9. To consider whether the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024 as drafted provides adequately for mutual international assistance in matters relating to computer-related crimes and for related matters.

10. To make recommended changes, if deemed necessary, to the Bills as drafted for further consideration by the Chief Parliamentary Counsel.

4. The Committee has the honour to report as follows:

The Committee scheduled and held meetings on the following dates:

Preliminary and First Meeting – Monday 8th April, 2024

Second Meeting – Monday, 22nd April, 2024

Third Meeting - Monday, 6th May, 2024

Fourth Meeting - Monday, 13th May, 2024

Fifth Meeting - Thursday, 23rd May, 2024

Sixth Meeting - Monday, 27th May, 2024, and

Seventh Meeting – Thursday, 4th July, 2024.

The Minutes of the meetings are appended hereto and marked "**A1" – "A7"** respectively and form part of this report.

All the meetings were held at the Parliament Buildings, Bridgetown.

5. A copy of the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024 which are appended hereto and marked **"B1"** and **"B2"** are available online on Parliament's website and the Government Printing Department's website.

6. The Committee in keeping with its parliamentary practice issued a Press Release inviting and encouraging the public whether as individuals, professional organisations, community-based groups, official and unofficial bodies with special interest and generally anyone who may assist with its work to submit memoranda or other documents setting out their views and comments on the issues.

7. The Committee invited submissions from the following organisations and persons:

- Democratic Labour Party
- Barbados Labour Party

- Rev Bishop Joseph Atherley
- Sir David Simmons, K.A., B.C.H., S.C., *Chairman of the Law Reform Commission*
- Mr Niel Harper, *Cyber Security Expert*
- Ms Stephanie Chase, *Educator and Blogger*
- Mr Kammie Holder, *Managing Director, Prudential Financial Sales & Services Inc*.
- Mr Peter Thompson, *Retired, CEO and Founder, Remote Work (Barbados)*
- Ms Marcia Weekes, *Self Employed, Step By Step Productions*
- Mr Steven Williams, *Principal Consultant, Data Privacy and Management Advisory Services*
- Mr Kemar Stuart
- Mr Anthony Clerk, The Barbados Bankers Association
- Starcom Network Inc.
- Barbados Bar Association
- Commissioner of Police, *Barbados Police Service*
- Barbados Today Newspaper
- Caribbean Broadcasting Corporation
- Nation Publishing Co. Ltd.
- Barbados Association of Journalists & Media Workers (BARJAM)

The Committee decided that written submissions should reach the office of the Clerk of Parliament no later than Friday, 25th April, 2024.

8. The Committee decided that the oral presentations should be ten (10) minutes in length followed by a question and answer session. The Committee heard oral presentations from the following persons and a summary of those submissions are available in the attached minutes to the Committee.

- Sir David Simmons, K.A., B.C.H., S.C., *Chairman of the Law Reform Commission*
- Mr Niel Harper, *Cyber Security Expert*
- Mr Steven Williams, *Principal Consultant, Data Privacy and Management Advisory Services*
- Mr Anthony Green, *General Manager – Starcom Network Inc*
- Mr Kemar Stuart
- His Excellency Rev Dr. Ferdinand Nicholls, ORDM
- Ms. Janine Butcher, *Customer Service Representative*
- Mr. Victor Lewis, *Retired Police Officer and Educator*
- Ms. Heather Cole, *Budget Analyst, New York*
- Mr. David Weekes, *Retired*

- Mr. Timon Howard, *Student, University of the West Indies (UWI) (Cave Hill) and Spoken Word Artist*
- Hon. Ms. Marsha K-A. Caddle, MP., *Minister of Industry, Innovation, Science and Technology*

9. Technical Support was provided by Ms Rhea Drakes, Parliamentary Counsel, Office of the Chief Parliamentary Counsel (CPC).

10. We think it is important to note that these Bills were submitted to the Committee but not in the usual manner. This prompted commentators to remark that the process was flawed. Former Senator Caswell Franklyn was in the forefront with this accusation and his comments were given prominence in the news media.

These Bills were debated and passed in the House of Assembly on the 8th February, 2024 and sent to the Senate. These Bills were given Notice of in the Senate on the 7th February, 2024 and were read a First time on said date. However, because it was determined that in the public interest a fuller discourse on the Bills should be undertaken, the Bills were referred to the Joint Select Committee (Standing) on Governance and Policy Matters and that the Committee be empowered to consider the merits and principles of the bills.

However, there was a procedural hurdle to overcome as these Bills had already passed the House of Assembly and it was unusual for a Joint Select Committee (Standing) comprising members of that House to again reconsider a matter on which those Members had already come to a conclusion.

Standing Order 28(4) under the rubric "Rules of Debate" provides as follows:

It shall be out of order to reflect on any vote of the House or attempt to reconsider any specific matter upon which the House has come to a conclusion during the current session except upon substantive motion for rescission.

11. Parliament prepared the following note for the Chairman in response to the critics of this approach and for explanation of the process which was pursued:-.

Brief prepared by the Clerk of Parliament to the Chairman, Mr Edmund G. Hinkson, SC., MP. on the Response to Comments made by Former Opposition Senator, Mr Caswell Franklyn

Good Afternoon fellow Committee members, I feel constrained to respond to comments, appearing in the Daily Nation of April 25 under the headline "Caswell knocks Sir David", attributed to Mr. Caswell Franklyn a former Opposition Senator in this very space we now occupy.

I do not need to defend Sir David who was a guest of this Committee for comments made in relation to Sir David's contribution to the work of this Committee, Sir David is eminently qualified to do that.

However, Mr. Franklyn is quoted as saying "So they are reflecting on that Bill contrary to the Standing Orders ..." Further in the article in a reference to Sir David Simmons who as I cited earlier appeared before this Committee, Mr. Franklyn says "he should know the Standing Orders of the House and the Standing Orders do not allow this monstrosity that they have calling a Joint Select Committee."

Mr Franklyn continued, "The Joint Select Committee is a creation of this Parliament. It has never happened in Westminster system before where a Bill is passed in the Lower House, it goes to the Upper House and the Upper House then forms a Joint Select Committee. It is contrary to the rules of the House because once the House has passed it the House cannot go back into Committee on that Bill."

Let me here note that the House is not going back into Committee on the Bill but a few of its Members are sitting with Senators on a Joint Select Committee (Standing). More on this point later in my presentation.

Mr Franklyn added, "What should have happened - the Bill was passed in the House and then it should go to the Senate and if the Senate had problems, the Senate could identify these problems and send it back to the House or they could have formed a Committee of the Senate to investigate the Bill."

Standing Order 48(1) of the Standing Orders of the Senate empowers the Senate to commit a Bill to a Select Committee a fact which Mr. Franklyn acknowledges. And the Senate has so committed the Bills to this Joint Select Committee (Standing).

Mr. Franklyn is alleging that the Bill having passed the Lower House it goes to the Upper House where that House forms a Committee. For Mr. Franklyn's elucidation, the Senate did not form any Committee. The Senate as allowed by its Standing Orders, referred the Bill to the Joint Select Committee (Standing) on Governance and Policy Matters. Parliament had established these Joint Standing Committees in 2023. The House on the 2nd May, 2023 and the Senate on 17th May, 2023.

In the President's Address of 2022, (formerly known as the Throne Speech), the first under our new fledging Republican Status, the Government signalled its intention to embark upon an enhanced system of Parliamentary Committees, "An enhanced system of Committees of Parliament aimed at effecting wider national discussion and greater consultation with citizens on proposed legislation and Bills."

Three Joint Select Committees on, Governance, Economic issues and Environmental matters were established in both Houses.

Engaging citizens is a core business of the 21st Century Parliaments and Parliamentarians. Sustainable Development Goal 16 (SDG16) has two targets that refer to the role of Parliaments:

Target 16.6 Develop effective, accountable and transparent institutions at all levels;

Target 16.7 ensure responsive, inclusive, participatory and representative decision at all levels.

The creation of the Standing Committees, one of which is this Committee goes a long way towards satisfying the two targets set in SDG16. It also satisfies the commitment of the

Government as expressed in the Charter of Barbados for the development of active citizenship to deepen the effectiveness of our democracy.

In 2020, the OECD collated evidence and data supporting the idea that citizen participation in public decision making can better deliver policies, strengthen democracy and build trust. The report listed the seven point cited below:

1. Can lead to better policy outcomes because deliberation results in considered public judgments rather than public opinions, resulting in informed recommendations about issues;
2. Give decision makers greater legitimacy to make hard choices;
3. Enhance public trust in government and democratic institutions by giving citizens an effective role in public decision making;
4. Signal civic respect and empower citizens;
5. Open the door to a much more diverse group of people, making governance more inclusive;
6. Strengthen integrity and prevent corruption by ensuring that groups and individuals with money and power cannot have undue influence on public decision;
7. Help counteract polarization and disinformation.

I now turn to the real issue which to my mind Mr. Franklyn referenced; that of reflection by the House on the Bill contrary to the Standing Orders of the House of Assembly.

Standing Order 28(4) of the Standing Orders of the Honourable the House of Assembly provides as follows: "It shall be out of order to reflect on any vote of the House or attempt to reconsider any specific matter upon which the House has come to a conclusion during the current session except on a substantive motion for rescission." The argument here being that the Lower House had come to a conclusion on this matter and therefore it was contrary to the Standing Orders for the House to be seemingly reopening this matter.

Mr. Franklyn asserts that it had never arisen in the Westminster system that we practice, I cannot so assert because I have not researched that fact. However what Mr. Franklyn is ultimately seeming to suggest is that if it had, there is nothing the Parliament could do about it.

I first refer Mr. Franklyn to a judgment of the Supreme Court of the United Kingdom given by Lady Hale and Lord Reed. This case had to do with advice given by the Prime Minister to Her Majesty the Queen on 27th or 28th August, 2019, that Parliament should be prorogued from a date between 9th and 12th September until 14th October was lawful. It arises in circumstances which have never arisen before and are unlikely to arise again. It is a "one off". The court asserted that our law is used to rising to such challenges and supplies us with the legal tools to enable us to reason to a solution.

In our instant case one such tool in Parliamentary law as it were, is that the House can regulate its own procedure known as Exclusive Cognisance. Exclusive Cognisance simply put is the right of each House to judge the lawfulness of its own proceedings.

In a 1999 Joint Select Committee Report of the United Kingdom Parliament on Parliamentary Privilege under the Chapter 'Control by Parliament over its Affairs' the Committee had this to say:

> *Both Houses have long claimed, and succeeded in maintaining, the right to be sole judges of the lawfulness of their own proceedings and to determine, or depart from, their own codes of procedure. Courts of law accept Parliament's claim that they have no right to inquire into*

the propriety of orders or resolutions of either House relating to their internal procedure or management.

Speaking in his judicial capacity in 1974 Lord Morris of Borth-Y-Gest stated:

The question of fundamental importance which arises is whether the Court should entertain the proposition that an Act of Parliament can be so assailed in the Courts that matters should proceed as though the Act or some part of it had never been passed…. which doctrine would be dangerous and impermissible. It is the function of the Courts to administer the laws which Parliament has enacted. In the processes of Parliament there will be much consideration whether a Bill should or should not in one form or another become an enactment. When an enactment is passed there is finality, unless and until it is amended or repealed by Parliament…

It must surely be for Parliament to lay down the procedures which are to be followed before a Bill can become an Act. It must be for Parliament to decide whether its decreed procedures have in fact been followed. ***It must be for Parliament to lay down and to construe its Standing Orders and further to decide whether they have been obeyed; it must be for Parliament to decide whether in any particular case to dispense with compliance with such orders.*** *(my Emphasis)*

This ancient right remains of fundamental constitutional importance. The exclusive right of the two Houses to make and to vary their own rules of Procedure protects the legislative supremacy of Parliament and the exclusive right of the Commons to grant aids and supplies.

Parliament exercised such right in the instant case and passed on the 16th February, 2024 the following Resolution cognizant of the constraint placed upon it and course of action it would follow in having this Bill referred to the Joint Standing Committee. This followed a Resolution of the Senate which committed these Bills to the Joint Select Committee (Standing).

THE HONOURABLE THE SENATE

RESOLUTION

WHEREAS the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024 have been read a first time in the Senate;

AND WHEREAS it is in the public interest that a fuller discourse on the Bills be undertaken;

BE IT RESOLVED that subject to the concurrence of the Honourable the House of Assembly that the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024 be referred to the Joint Select Committee (Standing) on Governance and Policy Matters;

AND BE IT FURTHER RESOLVED that the Committee be empowered to consider the merits and principles of the Bills and report three (3) months from reference.

APPROVED by the Senate this 14th day of February, Two Thousand and Twenty-four.

Rill Fal

President

THE HONOURABLE THE HOUSE OF ASSEMBLY

RESOLUTION

BE IT RESOLVED that this House concurs with the Honourable the Senate that the Cybercrime Bill and Mutual Assistance in Criminal Matters (Amendment) Bill, 2024 be referred to the Joint Select Committee (Standing) on Governance and Policy Matters;

AND BE IT FURTHER RESOLVED that Standing Order 28(4) of the Standing Orders of the Honourable the House of Assembly be suspended for the duration of the deliberations of the Committee on the Bills and any matters connected thereto;

AND BE IT FURTHER RESOLVED that the Committee be empowered to consider the principles and merits of the Bills and to report no later than three months from the date of its reference.

APPROVED by the House of Assembly this 16th day of February, Two Thousand and Twenty-four.

Speaker

12. The process followed in this particular Bill though unusual is not the monstrosity as alleged by Mr Franklyn. As we have asserted, Parliament has the right to regulate its own procedure and in that regard suspended the operation of Standing Order 28(4) of the Standing Orders of the House of Assembly to allow the Members of the Lower House who comprise the Committee to participate in the work of the Committee for the duration of the life of that Committee.

The Senate did not form any Committee as suggested by Mr Franklyn but committed the Bill, as it is empowered to do under the Standing Orders, to the Joint Select Committee on Governance and Policy Matters.

Finally, this Committee is part of the enhanced parliamentary Committee architecture aimed at improving the way Parliament functions and I repeat what the President in her 2022 Address stated, "Good governance is pivotal to maintaining public trust and confidence and convincing members of the public that the political process and public institutions work in their best interests."

13. These Bills, particularly the Cybercrime Bill, 2024 excited public interest that led to over forty-eight (48) written submissions addressed to the Committee.

This interest solidified the decision to establish these Joint Select Committees (Standing), the establishment of which has as its core active citizenship and a deepening of our democracy. Engaging citizens is a core business of the 21st Century Parliament and satisfies Sustainable Development Goal 16 (SDG16), developing accountable and transparent institutions at all levels and ensuring responsible, inclusive, participatory and representative decisions making at all levels.

The majority of the submissions to the Committee highlighted issues relating to freedom of expression, vagueness of the language as it related to the offences, the broad nature in which the language is written and the uncertainty as to whether or not the terms can be objectively identified by the members of the public as something that is criminal.

One of the main criticisms to the Cybercrime Bill is the concern over an apparent curb in the freedom of expression. The Commission by a majority, held the view that the right to freedom of expression is not a right given in absolute terms. The Barbados Constitution at Section 20 provides for laws to be passed to limit that expression, provided that those limits are reasonably required in the public interest and also to secure the rights and freedom of others.

The intent of the Bill is not to unduly restrict people from expressing themselves, but from doing so in a manner by way of electronic means, on the internet that would interfere with other persons, or is likely to cause harm or effect change in the conduct of persons by way of some malicious or offensive actions.

14. WRITTEN SUBMISSIONS

The Committee received written submissions from the following:

1. Mr Niel Harper
2. Mr Steven Williams
3. Barbados Consumer Empowerment Network
4. David Weekes
5. Hugh B. Shepherd
6. Chesterfield St. C. Browne
   (i) 2nd Submission
   (ii) 3rd Submission
7. Kammie Holder
8. Donna Every
9. Melissa A. Goddard
10. Judy M. Driscoll
11. Hugh Patrick Greene
12. Theresa Annel
13. Margaret G
14. Valerie Hoyte
15. Mervin Marius
16. Peter Thompson
17. Peter Earle
    (i) 2nd Submission
18. Solutions Barbados; Grenville Phillips II
19. Yokaana Moore
20. Jeanie Mottley
21. John Lloyd
22. jazzmal2023@outlook.com
23. Sheldon Mottley
24. Rosaline Corbin
    (i) 2nd Submission
25. Dave & Marcia Weekes
26. Michelle Bayley
27. Lisa M. Niles
28. kmk2021biz
29. kgbusiness@caribsurf.com
30. Heather Cole **(Citizens of Barbados)**
31. Marcia Weekes
32. Timon Howard

33. Cecelia Bourne
34. Michael Bourne
35. Thierry Gittens
36. Lisa Niles
    (i) 2nd Submission
37. Cindy Benn
38. Dr. Philip Corbin, Family-Faith-Freedom, Barbados
39. Carlyle Sylvester Edwards
40. Kally B
41. Lisa Niles (Petition)
42. Cecelia Bourne (Erratum)
43. The Barbados Police Service (TBPS)
44. Mr Niel Harper, (oral presentation)
45. The Barbados Bankers Association (TBBA)
46. The Barbados Bar Association (BBA)
47. Barbados Association of Journalists and Media Workers (BARJAM)
48. Office of the Director of Public Prosecutions (DPP)

The written submissions are appended hereto and marked **"C1" – "C48"** and form part of this Report.

15. For the purposes of this Report a succinct summary of some of those forty-eight (48) submissions are provided here not necessarily in the order cited earlier. All were not commented upon here because there were either one or two liners or repeated some of the comments listed here.

David Weekes welcomes the initiative of the government to bring the Cybercrime Bill, 2024. However, he sees the deficiencies in the form of Clause 19 which speaks to "intimidation" as grounds for cyber protection. He also makes reference to ridicule contempt and embarrassment as grounds for an offence in the cyber world. He reasons that ridicule, contempt and embarrassment and others as he deems them social emotion, to use them as a means of criminal deviance is extreme and should be struck from the Bill.

The Barbados Consumer Empowerment Network expressed strong support for the inclusion of protective provisions for consumers using digital financial platforms. That organisation is of the view that explicit provisions to protect and safeguard consumers in the digital age are needed.

It further stated that though the Bill indirectly facilitates customers, it does not explicitly focus on the digital finance protection for consumers; nor does it focus on redress or penalties for digital financial crimes against consumers.

Mr. Hugh B. Shepherd cited that there were two (2) clauses of the Cybercrime Bill, 2024 that are contrary to the Universal Declaration of Human Rights/ and/or International Human Rights Law.

Mr. Shepherd referenced Clause 19.(3):

"A person who intentionally uses a computer system to disseminate any image or words, not caring whether they are true or false, and causes or is likely to cause or subject a person to ridicule, contempt or embarrassment, is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both."

He proffers that this clause contravene freedom of expression as expressed by the United Nations.

"Everyone shall have the right to hold opinions without interference" and "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and input information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."

Clause 19.(5) *"The defences of truth, comment, triviality and privilege whether absolute or qualified, provided for under the Defamation Act, Cap. 199 shall extend to a prosecution under subsection (3)."*

Mr. Shepherd opines that the clause as drafted ran afoul of Human Rights. He further claims that International Human Rights Law provides that individuals should have the right to a legal remedy for defamation.

Mr. Chesterfield St.C. Browne criticised the Parliamentary process that was followed. He is of the view that the Cybercrime Bill, 2024 could have followed the usual Parliamentary process of Bills, starting in the House, progressing to the Senate and not the Joint Select Committee route that was chosen.

As was stated earlier, Parliament is at liberty to regulate its own procedure under a rule call, "Exclusive Cognisance" and the route of the Joint Select Committee is such an option available to the Parliament.

Mr. Browne in his actual criticism of the Bill cited Clause 20.(1), addressing its vagueness with respect to exclusion for artistic expression and satire.

Vagueness of Terms

He listed an example of such vagueness – he referenced the list of offensive characteristics for data is subjective and open to interpretation. What one person finds offensive, another person might not. Mr. Browne feels that vagueness can lead to unintended and undesirable consequences for the citizens of Barbados. These undesired outcomes include but that are not limited to:

1. A chilling effect on free speech as citizens of Barbados might be afraid to express themselves online for fear of prosecution.
2. Unequal application of the law depending on the interpretation of "offensive" by law enforcement or the court.
3. Clauses 23.-28. reveals that broad powers of search and seizure without the requisite checks and balances.
4. The absence of clear legal basis for data seizures. The view is expressed that the Bill fails to address situations where the malicious actors (hackers and scammers) might plant data on a user's device without their knowledge or consent.
5. Lack of expertise - Lack of qualifications for police officers handling seized data raises concern about potential mishandling of evidence or data breaches.
6. Self incrimination.
7. Data corruption.
8. Limited oversight.

Mr. Browne concluded that a well-drafted Cybercrime Bill, 2024 should strike a balance between protecting citizens from online threats and safeguarding fundamental rights. Good legislation is characterized by clarity, precision and due process. Vague terms like "offensive" can lead to misinterpretations and unusual application granting law enforcement officers broad search and seizure powers without proper oversight mechanisms undermines citizen trust and creates opportunities for abuse.

Donna Every felt that the Cybercrime Bill, 2024, rather than focusing on cybercrime could be used to make freedom of speech and freedom of religious beliefs a crime if a writer uses words that may cause "annoyance, embarrassment, insult or emotional distress." She questioned the very broad definitions in the proposed legislation which left room for misinterpretation.

Kammie Holder posited the view that most reasonable Barbadians accept the need for modern cyber laws to mitigate malicious actors. He posited the view that Clauses 19., 20. and 21. need reforming. He questioned what defence was open to him if someone claimed annoyance, embarrassment, insult, reputational injury, emotional abuse and intimidation by

what he said. He wondered why there were no provisions for warning of a first offender rather than summary and indictable offences.

Melissa A. Goddard recommends that the Cybercrime Bill, 2024 should be significantly amended, redrafted or be completely withdrawn and replaced with better-drafted legislation. She is of the view that having someone dislike you because of something they heard or feeling embarrassed or offended because of something posted on the internet is not an adequate benchmark or legal reasoning to limit someone's right to free speech or expression. She was of the view that a Bill cited as 'Cybercrime' is not the ideal place to locate such crime.

She feels that the legislation strikes at the very heart of freedom of speech and expression. The legislation needed to be drafted more lightly and that more precise language be employed.

She posits that the Bill wanders through many different uses of the internet – from issues of privacy, bullying, terrorism, revenge porn, hacking, libel, disinformation and more – and yet never fully lands or properly deals with any of them is what is objectionable. The writer advances that not even the new emerging technology of A.I. was addressed.

Judy M. Driscoll's concern related to Clause 19.(3) where in her view the Cybercrime Bill, 2024 was seeking to make illegal what is now legal merely because it was being said on a computer or smart device. She felt this should be amended.

Hugh Patrick Greene described himself as an electrician, computer technician and an independent software developer for Windows and Linux Operating Systems. He strongly objects to the Cybercrime Bill, 2024 as presently drafted. He felt the language with respect to the offence was too vague and often open to misuse and abuse.

He relied on Wikipedia's definition of cybercrime as one covering a wide range of criminal activities that are carried out using digital devices and/or networks. These crimes involve the use of technology to commit fraud, identity theft, data breaches, computer viruses, scams and expanded up into other malicious acts.

In 2000, the 10th United Nations Congress on the Prevention of Crime and Internet Offenders placed cybercrime into the categories of: unauthorised access, damage to computer data or programme, sabotage to hinder the functioning of a computer system or network, unauthorised interception of data within a system or network, and computer espionage.

Theresa Annell zeroed in on the clause which seeks to penalise ideas because someone feels hurt or embarrassed by her words.

Valerie Hoyte argues that the Cybercrime Bill, 2024 affects free speech and having a Bill drafted so widely that it makes interpretation difficult is bad.

Mervin Marius feels that the Cybercrime Bill, 2024 in its present form will have a negative impact on churches and religious organisations. Groups can now threaten the use of hate speech because they can take offence to what is being said about one.

Peter Thompson asserts that the Cybercrime Bill, 2024 goes way beyond the parameters set by the Budapest Convention. He stresses that it is perversion of fundamental justice that lawful speech in-person suddenly becomes a criminal act when expressed online.

Peter Earle felt that it was essential for a balance to be struck between protecting individuals and upholding the fundamental rights of free speech and political expression. While it has been argued in defence of the Cybercrime Bill, 2024 that Barbadians are free to transmit data as long as it does not cause others distress, the Bill's language regarding emotional distress was vague and subjective.

The assertion that the Bill affords defences for truth, comment, triviality and privilege is not sufficient to allow concerns about its potential impact on free speech. There are concerns for bloggers, online commentary and on certainty over safeguards to protect freedom of expression.

Solutions Barbados, Grenville Phillips II; President. Their main concern is Clause 20. of the Cybercrime Bill, 2024 especially 20.(1) "publishing data that is offensive... for the purpose of causing annoyance or embarrassment."

He argues that in the *Computer Misuse Act* Cap. 124B which the Cybercrime Bill, 2024 seeks to replace is not as harsh. He felt that is not reasonable for politicians to be:

1. Embarrassed by publication of unfavourable statistics; and
2. Annoyed by repeated publications of statistics that could support accusation of their incompetence.

He suggested that the change in language from the *Computer Misuse Act* Cap. 124B (Section 14) to the Cybercrime Bill (Clause 20.) was to prevent Barbadians from commenting publicly on social media where such comments were likely to embarrass the government. To use his words, "it seems crafted to misuse a Bill originally intended to punish actual cybercrimes (like cyber terrorism and child pornography) and use it to intimidate Barbadians into silence through fear."

He is therefore suggesting that Clause 20.(1) of the Bill be replaced by Section 14 of the *Computer Misuse Act* Cap. 124B and omit Clauses 24.(1) and (2) which in his view appears to be a violation of civil and political rights.

Yokaana Moore feels that the Cybercrime Bill, 2024 violates rights to privacy, freedom of expression, and access to information online. It may give the government unprecedented power to monitor and control our online activities, potentially leading to censorship and surveillance of innocent citizens.

Ms. Moore cites the following reasons for her objections and opposition to the Bill. Threat to freedom of expression given its vague and broad language which criminalizes legitimate online activities including criticism of the government and peaceful dissent:

(a) Overreach of police powers.

(b) Cybersecurity threats: The experts have cautioned that it will weaken our defences by creating vulnerabilities despite Government's claim that it will enhance cybersecurity.

(c) International Reputation: Ms. Moore cites damage to Barbados' international reputation as a democracy that respects human rights and fundamental freedom.

She calls for the government to withdraw the Cybercrime Bill, 2024.

Mrs. Jeanie Mottley writes that the Cybercrime Bill, 2024 in its current form with regard to Clause 20.(1) cyberbullying will criminalize a person or group of persons. The clause uses troublesome language which is vague. She cites examples of cyberbullying which may prove difficult to establish: publication by online newspapers. She is suggesting that a glossary be attached to the Bill which clearly and succinctly explains the terms used to define cyberbullying

John Lloyd, whilst recognizing the importance of addressing cyber threats and the need for ensuring digital security, expressed a deep concern regarding the proposed Cybercrime Bill, 2024.

He fears that the Bill threatens to infringe upon our rights to privacy, freedom of expression and access to information online. There is concern that the Bill gives government unprecedented power to monitor and control citizens' activities with the potential of censorship and surveillance of innocent citizens.

Mr. Lloyd calls on the government to provide adequate safeguards for data privacy given the broad powers given to law enforcement agencies to access and seize computer data.

Sheldon Mottley opines that the Cybercrime Bill, 2024 offends the *Constitution of Barbados* and Articles 18 and 19 of the Universal Declaration of Human Rights of the United Nations.

He feels that the language of the Bill is too wide, vague and ill-defined. The Bill in his view will prohibit and muzzle all constructive criticism of the government as well as alternative proposal and options to what government may propose and that the Bill will intentionally or unintentionally stifle and muzzle the freedom of expression and opinion, and, movement and free association of Barbadians.

Mrs. Rosaline Corbin supports fully Clauses 16., 17. and 18. respectively relating to child pornography, child grooming and online sexual abuse.

Mrs. Corbin hopes that the other aspects of the Cybercrime Bill, 2024 are not seen as Barbados's desire solely to comply with international conventions.

She noted that seniors are vulnerable to cybercrime if their laptop/tablet is in need of repairs and they fall victim to some attack by the repairman. Who is then liable to be charged? Similarly, in respect of children who use their phones to post various images and stories, how will minors be treated under the law?

Michelle Bayley reviewed Clause 23.(2) and accepted that Barbados in order to combat the threat of cybercrime had to enact comprehensive cybercrime law.

She is, however, concerned with clause 23.(2) which grants to police officers broad powers during their cybercrime investigations. Whilst this provision is crucial for law enforcement, lack of technical expertise required to execute its mandate effectively and the potential for mishandling of personal data undermine these efforts.

In her view, Clause 23.(2) raises the issue of law and specificity for technical tasks. The tasks police officers are asked to perform and their lacking in the skill required, especially cryptography. Potential for evidence compromise, improper handling of digital evidence during data seizure or storage can lead to its exclusion from court.

The Bill is silent on a liability and remedy if accused persons' data is damaged in any way during the retrieval process by law enforcement.

<u>Her proposed amendments</u>:

Clause 23.(2)

(d) In consultation with a qualified cryptologist or computer forensic expert, have access to any information code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer system into readable and understandable format or test, for the purpose of investigating an offence.

Clause 23.(2)

(g) in consultation with a qualified data management specialist, maintain the integrity of the retrieved and stored computer data.

Ms. Bayley is recommending the establishment of protocols between police officers and specialists during investigations or the development of a national certification programme for police officers in the handling of digital evidence all aimed at striking that balance between efficient law enforcement and integrity of digital evidence.

Lisa Niles was concerned with Clause 19.(3) "Malicious communication".

Her statement of the clause "whether true or false" ignores the words preceding "not caring" and therefore she gives a different interpretation to the clause.

In keeping with a lot of the other concerns persons have had, Clause 19. is certainly one that has had its share of criticism.

Again, Clause 23. "Search and seizure" which gives wide powers to a police officer is cause for concern.

Ms Niles queried whether Clause 24. "Assisting a police officer" and the mandatory nature of the provision and wondered whether it was in conflict with other laws.

Ms Marcia Weekes has raised concern over Clauses 19. and 20. of the Cybercrime Bill, 2024 and their negative impact on public speech, opinion and dissemination of information. She posits that criminalization of freedom of expression whether true or false is a dangerous precedent being set by the government.

It is of no comfort to say that one has recourse to the law courts to prove one's innocence as there is a cost attached to such a course.

She is firm in her view that the intent of the Bill is to cause strife and hinder public speech and opinion.

Mr. Michael Bourne has taken issue with Clause 19.(5) pertaining to "Malicious communication". It strikes at the heart of freedom of expression and dissemination of information.

He cites the case of the Nigerian lady who was charged under section 24(1)(*b*) of the *Nigerian Cybercrime Prohibition* Act.

Mr. Thierry Gittens cautions that Clause 19.(8) may negatively impact the youth and he is concerned with the level of fines being levied when compared to other criminal charges.

Miss Candy Benjamin has highlighted concerns with respect to Clauses 19.(3), 19.(5), 20.(1)(*b*), 23.(1), 24.(1) and 26.(1).

Chesterfield Browne's concern is the legal implication of what he describes as deep fake technology on the application of the cybercrime Bill.

Deep fake technology is a computer software that uses artificial intelligence to create fake videos or audio recordings of people that look and sound exactly like the real thing period it is like a high tech version of impersonation or mimicry where the computer learns to mimic a person's face or voice.

For example, it could be used to make a video of a celebrity saying things that he or she never actually said or to make a fit phone call that sounds like it is coming from your friend. The technology is called "deep fake" because it uses "deep learning" (a type of artificial intelligence) to make the "fake" content. It is a powerful technology that can also be misused so it is essential to be aware of it.

Dr. Phillip Corbin, Chairman of Family-Faith-Freedom, Barbados lauds aspects of the Bill that seek to suppress child pornography, child grooming and online sexual abuse. However, it is that organisation's belief that the Bill in its current form lends to undermining the fundamental human rights of freedom of conscience and freedom of expression.

As has been the case of several commentators on the proposed amendments, Clauses 19. and 20. are the clauses that create concerns with respect to freedom of expression and very emotionally charged language and one that promotes too much subjectivity.

Kathy B's concern like other commentators is with Clauses 19.(1) and 20. and its threat to freedom of expression and the vague and subjective language to fraud criminal liability.

Kathy B asserts illegal access at Part II, the broad excessive powers of confiscation and access to computer systems is a concern of hers.

In Part III, Clause 26(1), the broad and intrusive powers given to law enforcement officers and repeats the call to revise the legislation.

The Barbados Police Service supports the introduction of the Cybercrime Bill, 2024 and feels that the Bill enacts the provisions of the Budapest Convention.

The Service feels that the new provisions found in Clauses 19. and 20. which replaced those of the *Computer Misuse Act* Cap. 124B and provide a more secure platform for law enforcement to investigate cyber-related crimes reported to them.

The Service also reflects on the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024 which in their view recognised the need for cooperation between States and private industry.

They highlight that the provisions recognise that the fight against cybercrime requires speed, agility and cooperation in criminal matters and are in line with Articles 25-34 of the Budapest Convention.

Barbados Bar Association (BAR), in its Executive Summary to its report to the Committee, recognizes the importance of establishing a statutory regime to provide rules of conduct and acceptable modes and understanding and standards of behavior for the use of the internet, computers and related digital technologies.

The BAR feels it is equally important that a balance be struck between the above and the safeguarding the fundamental rights and freedoms of the citizens of Barbados, namely freedom of speech and expression as enshrined in the Constitution.

The BAR posits that the public of Barbados is entitled to expect a responsible and proper exercise of public power, which is fundamental to the operation of the rule of law. They concluded that up to the date of the submission of their report, the level of debate and interrogation of this Bill had been inadequate. The BAR opined that unless amended the Cybercrime Bill, 2024 will inevitably face challenge in the courts. It therefore:

(i) cautions the framers to consider the language of the Bill, in particular where it may have the effect of imposing legal terms which heretofore did not exist in the country's legislative framework;

(ii) recommends a careful examination of the powers proposed to be conferred, the rules of evidence and the criminal procedure, and other criminal justice matters in the Bill;

(iii) re-examines the unintended consequence of the proposed repeal of Section 34 of the *Defamation Act*, Cap. 199.

The BAR was particularly concerned with Clause 19 and more specifically Clause 19.(3) and its constitutionality. Indeed, a very large part of the submission was devoted to the issues raised by that clause and are fully distilled in their document which is appended and forms part of this Report

The Barbados Bankers Association Inc. (TBBA) commented on the Cybercrime Bill, 2024 in this way:

> *With respect to receiving or giving access to computer programs or data the TBBA feels that greater protection should be afforded to the publishers whose platforms may be used for such purposes despite prohibition against the same, provided that the publishers are not negligent in removing the offending material.*

Clause 19. *Transmitting data which causes substantial emotional or distress.*
The TBBA's view is that wide nature of this provision would seemingly endanger the Bank's ability to transmit correspondence to a customer that advises him that enforcement action may follow if a facility is not repaid by the certain deadline.

Clause 20. *Cyber bullying*
This Clause was felt to be unduly wide and had the potential to impact a Banks' communication of negative news to its customers.

Clause 22. *Aiding and abetting*
The view was expressed that there should be clear protection for employers whose employee or contractor uses his work email address or Bank issued device to distribute or commit an offence that is outside of his duties.

Clause 23.(2)*(d)*
This Clause should include protection for "privilege information or material" as is done under the *Proceeds and Instrumentalities of Crime* Act, 2019.

Clause 26.(2) *Production of data for criminal proceedings*

This clause is wide and prevents any disclosure of any information. It may instead have been intended to prevent tipping-off and should be reworded.

<u>Scope of the words "without authority" in the Cybercrime Bill, 2024</u>

It was recommended that there be a definition which confirms the scope of those words to ensure that persons acting in accordance with consent, legal or contractual basis, on the basis of professional advice or in good faith are protected.

NB "without authority", has been defined in the proposed amendments recommended by the Committee.

Mr. John Moore whilst recognizing the importance of addressing cyber threats and the need for ensuring digital security expressed a deep concern regarding the proposed Cybercrime

Bill, 2024. He fears that the Bill threatens to infringe upon our rights to privacy, freedom of expression and access to information online.

There is concern that the Bill gives the government unprecedented power to monitor and control citizens' activities with the potential of censorship and surveillance of innocent citizens. Mr. Moore calls on the government to provide adequate safeguards for data privacy given the broad powers given to law enforcement agencies to access and seize computer data.

Change.org - Petitions to the Committee.

The group citing fundamental principles established by the Human Rights Council quoted as follows: "same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice".

On the above basis, the group expressed the following concerns with regard to the Cybercrime Bill, 2024.

1. Broad powers. They opined that the courts and law enforcement officials were given extensive powers to seize individuals' computer devices and could compel access under the threat of charges for non-compliance.
2. Courts and law enforcement officials can compel telecom companies or Digicel and Flow to provide locations from cell towers, internet browsing activity and metadata from phone calls without the sufficient legal justification.
3. Breach of consumers' privacy as it relates to data and the misuse of that data.
4. The penalties under the Bill are harsh with fines of up to $70,000 or seven (7) years' imprisonment.
5. The vague use of language as it relates to offences.
6. The government being granted significant surveillance authority and without adequate checks and balances could lead to law enforcement overreach.
7. To safeguard Article 15 of the Budapest Convention demands conditions and safeguards for the adequate protection of human rights period.
8. Impartial tribunals should be established to implement the Bill's provisions.
9. The group cited abuse of cyber freedom that were recorded as in parts of the world not known for stellar human rights record.

It then called upon the government to amend the Cybercrime Bill, 2024 in the following manner:

1. Eliminate ambiguity and provide clear definitions; and
2. Prevention of the stifling of freedom of expression.

Office of the Director of Public Prosecutions (DPP)

The DPP weighed in on the Cybercrime Bill, 2024 and agreed that the Bill was both timely and necessary given the speed and anonymity of the internet that allows criminals to commit a range

of crimes from large scale cyber-attacks to activities such as using malware, phishing and spam and the facilitation of serious organised crimes through the use of technology.

The Office drew attention to the controversy surrounding Clauses 19 and 20 which established offences of malicious communications and cyber bullying respectively.

The Office referenced the Barbados Bar Association's report to the Committee which identified possible constitutional infringement resulting from the wording of Clause 19 (3) of the Bill.

The Office agrees that the word "embarrassment" under Clause 19.(3) of the Bill is an unlawful restriction on the right to freedom of expression. The Office holds the view that in the sphere of malicious communications, embarrassment has never been a base for criminal action against a person. Historically, a malicious communication was one which exposed a person to hatred, contempt and ridicule. A threat to the person's life was also required.

The *Computer Misuse Act,* Cap. 124B

Objectively, the communication must cause the recipient or any other person to whom the sender intends the communication to be sent some annoyance, inconvenience, distress or anxiety.

The Office asserts that the opposition to clauses 19 and 20 has constitutional dimensions as these offences make it likely that the fundamental right to freedom of expression will be contravened

They call in aid, Professor Thomas I. Emerson's assertion on the system of freedom of expression of the four (4) premises upon which the system of freedom of expression is based:

1. Freedom of expression self-fulfilment;
2. It is an essential tool for advancing knowledge and discovering truth;
3. It is a way to achieve a more stable and adaptable community; and
4. It permits individuals to be involved in the democratic decision- making process.

The Office holds the view that Clause 20. of the Bill criminalizes the intentional use of a computer system to publish, broadcast or transmit data that is offensive, indecent or menacing in character for the purpose of causing humiliation, embarrassment and other things.

Section 20 does not offend the Constitution because the offence seeks to prohibit the dissemination of morally outrageous expressions. And, as with such restriction, would be reasonable required in the interest of public safety and public morality.

The Bill has introduced several key offences which serve to enhance cybersecurity and to address some contemporary societal issues. The Bill prohibits cyberbullying child pornography, child grooming, cyber-terrorism, online child sexual abuse and revenge pornography. Law enforcement officials will be gladdened by these additional offences as they related to crimes committed against vulnerable persons.

The Constitution of Barbados guarantees to every resident of the country the right to the enjoyment of his freedom of expression which includes the freedom to hold opinions without interference, freedom to receive ideas and information, and freedom to disseminate information and ideas without interference (Whether the dissemination be to the public or to any person or clan of persons and freedom from interference).

In a system of governance founded on constitutional democracy, it is imperative that the competing interests of the State and of the individual are reconciled. This right is subject to lawful restrictions that are reasonably required in the interests of defence, public safety, public order, public morality or public health.

With respect to the use of the word embarrassment, an examination of the case law revealed that has never been a basis upon which criminal liability is founded.

Given the current draft of Clause 19.(3) it is understandable that certain sections of the public may interpret the actions of the State as seeking to silence public dissent. The law historically never criminalizes acts that had the potential to embarrass or humiliate persons. In relation to criminalize speech, the law is concerned with acts which cause a person to apprehend the immediate application of unlawful force or those which actually cause a person to suffer a (recognised) psychiatric illness.

16. Sir David Simmons, KA, B.C.H., S.C., Chairman of the Law Reform Commission

Given Sir David Simmons' position as Chairman of the Law Reform Commission and his central role in the current draft of the Bills under consideration the Committee formally invited Sir David Simmons, to make a presentation to the Committee on the Bills.

He began his presentation with a quotation from the judgement of Mr. Justice Frank C. Persaud in the High Court of Trinidad and Tobago on the 26th October, 2015 in the case of *Theresa Ho v. Lendl Simmons*, former West Indies cricketer.

That quote is worth repeating because it was the perfect platform for the discussion of the Cybercrime Bill, 2024. At paragraph 35 of the judgement:

> *The impact of social media and its consequent effect on our individual and collective privacy has to be acknowledged and addressed. There is a tendency for persons to hide behind a perceived anonymity that comes from using a username and or user profile while sitting behind a computer screen or using a handheld device to engage in offensive, hurtful, divisive and destructive this course. These persons may feel that they are empowered but their actions can infringe upon the rights of others with the aggrieved person having no recourse.*

At paragraph 36 of the judgement, in the respect of online conversations he observed as follows, "the impact upon an individual's privacy is tremendous and absence of clear and cohesive legislation to protect our citizens' privacy and to punish those who violate the rights of

others, can cause us to descend into a bottomless pit of anarchy. The time for legislative intervention is long overdue."

Sir David went on to cite the Sunday Sun editorial which wrote *inter alia*, "truth be told, some regulation is needed in Barbados if only to:

1. *Protect our children from those who will wish to do them harm through sex, manipulation and violence*
2. *Hold people accountable for what they may say about others.*
3. *Shield consumers from unscrupulous business practices.*
4. *Protect our constitutional rights to privacy and the maintenance of people's good name. The internet is invaluable but it does not provide an avenue to shout 'fire' in a crowded place when there is no just cause.*

He then referenced the *Computer Misuse Act* of 2005 of some 19 years' vintage. He stated that it was accepted by all sides and those holding themselves out to be experts in the area that the *Computer Misuse Act* is outdated because the march of technology and the variety of computer systems have made it antiquated.

Secondly, the Act was far too narrow in scope to be an effective tool for the police and prosecutors to cope with contemporary criminals and the variety of cybercrimes that have spawned since 2005.

Sir David Simmons was quick to point out that the Cybercrime Bill currently engaging the attention of the Committee is the legal measure adopted by the Government of Barbados to establish certain criminal offences under our domestic law with the Articles of the Budapest Convention as the benchmark against which the provision of the Bill was to be tested. He asserted that it was not a response to the plea of Justice Frank Seepersad earlier cited.

In light of the public criticisms of the Bill, he was authorised by the Law Reform Commission to discuss those criticisms to and determine if there was any validity to such criticisms.

Freedom of expression; freedom of speech under the Constitution:

The specific individual right of the concern to the Committee through this Bill, is that of freedom of expression. That can be found expressed in Section 20 of the *Constitution* which Sir David described as in two parts as it were. In the first part he cited as it were the actual right, the imperative in his view, and in the second part which he deems as derogating from the first part.

Section 20. (2) of the Constitution provides as follows:

> *"Nothing contained in or done under the authority of any law should be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provisions-*

(a) That is reasonably required in the interest of defence, public safety, public order, public morality or public health; or

(b) That is reasonably required for the purpose of protecting the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts or regulating the administration or technical operation of telephony, telegraphy, posts, wireless broadcasting, television or other means of communication or regulating public exhibitions or public entertainments; or

(c) That imposes restrictions upon public officers or members of a disciplined force.

The right and freedom of expression is not absolute. It is with regard to the criticisms of Clauses 19.(1), 19.(2) and 19.(3). The response of the Law Reform Commission is that the Bill satisfies Section 20.(2) of the *Constitution* because it is reasonably required in the interest of public morality, order and also from the point of view of protecting people's reputations in defamation cases.

Secondly, the Bill cannot be unconstitutional to the extent that it requires *mens rea* for several offences. There are twenty-three (23) times when the phrase "intentionally or recklessly or intentionally and sometimes without authority" is used. It is a protection against arbitrary conduct being criminalized. If a defendant can show that he did not act intentionally or recklessly, he has a good defence on all of those charges.

In respect of 19.(3), the Bill incorporates specific defences from the *Defamation Act,* Cap. 199 in Clause 19.(5) of the one of the few Bills to be, it does not threaten freedom of speech. What it does is to emphasize to citizens who may use computer systems, that if they transmit data provided that is not offensive in law or injuring the feelings or reputations of others, they can transmit their data freely, subject to limitation.

One therefore had to test the Bill against Section 20.(2) of the *Constitution* in that it was not unconstitutional in that it imposes limitations on the interest of public morality, public order or for the purpose of protecting reputations and so on.

Child pornography- defence available of bonafide research.

Child grooming is a new offence but it, again, is committed if a person intentionally or recklessly using a computer does these things.

Every offence requires proof of *mens rea.* The legislation does not contain any offence of strict liability. Throughout the Bill, defences are *mens rea* provided within the definitions as well as defences separate and apart. So, words such as "*intentionally recklessly or without authority*", the offences which relate to access to the computer, breaking into a person's computer or getting people's passwords, it has to be done without authority to constitute an offence.

Child sexual abuse is where a person intentionally or recklessly uses a computer system to meet a child for the purpose of engaging in sexual activity with a child or where an inducement, force or threat is used.

With respect to cyber bullying at Clause 20.(1) is where;

A person intentionally uses a computer system to

(a) publish, broadcast, or transmit data that is offensive, pornographic, indecent, vulgar, profane or of a menacing character, or causes such data to be so sent;

(b) for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or cause substantial emotional distress...

Another criticism of the legislation is that language used outside of your computer is not criminal but so long as it is done *via* the computer it is. This presented a difficult question to the Committee. In other words, if I can annoy somebody, embarrass and humiliate them without the use of a computer and I can do it lawfully what makes it unlawful merely because a computer is used to commit the act?

Sir David said that our proposed legislation is in harmony with the Conventions (Budapest is the one that is enforced) notwithstanding that the UN may be working on one now.

Once Barbados passes the cybercrime legislation it will enable Barbados to accede to the Convention and get the benefits of the Convention.

Sir David then addressed his mind to the terms of reference under which the Committee worked:

1. "To enquire into and determine whether the Cybercrime Bill as drafted fulfils the expressed purposes to ensure compliance with the International Conventions, global standards and best practices to counter cybercrime and to ensure international cooperation in the combatting of cybercrime." Overwhelming yes, the Council of Europe proclaimed that our legislation is the best contemporary legislation in the region.

2. Secondly, "to examine whether the Cybercrime Bill as drafted curtails the citizens' fundamental rights to freedom of expression as against the protection of the reputation, rights and freedoms of other persons or their private lives." Sir David answered in the negative and reiterated that it does not curtail citizens' fundamental rights. It rather enhances the protection of reputations as envisaged in the Constitution.

3. "To examine whether the Cybercrime Bill as drafted provides the necessary checks and balances, safeguards and independent oversight to protect citizens' human rights, liberties and privacy rights from potential abuses, including from expansive law enforcement powers in order to prevent miscarriages of justice." Sir David indicated that the Bill does not safeguard or provide independent oversight to protect human rights. That is not the function of the Bill. That is the function of the various independent human rights NGO's.

4. "To examine whether the Cybercrime Bill as drafted provides adequate protection to all of the specific categories of persons who may potentially be vulnerable to cybercrime."

Sir David stated that as far as we can see the Bill provides adequate protection for the various categories of persons to whom the clauses are directed.

5. "To examine whether the penalties imposed in the Cybercrime Bill as drafted are disproportionate and/or unreasonable in any way". Generally, the response we gave and having regard to similar legislations elsewhere, Sir David could not agree that the language used was vague and uncertain in its application notwithstanding two instances being referred to CPC for review.

6. "To examine whether the Cybercrime Bill as drafted provides adequate protection for whistle-blowers who expose cyber-related wrongdoing and, if not, whether such protection is provided in any other legislation". Sir David pointed to the metrics of fines and penalties from around the region. It would be for the Committee to make a determination on that. Sir David reiterated what he said at the outset, that the function of the Law Reform Commission was to draft legislation and submit to the government. The government's job was to implement. With respect to whistle-blower legislation, that was enacted in 2022.

7. "To consider whether the Bill could impede innovation in the technology sector and discourage investment and research in digital infrastructure." Sir David could not answer. His Commission could give no answer. This was for the people engaged in technology connected to cybercrime and cybersecurity to answer.

With respect to the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024: this legislation goes back to the late 90s. The amendment provides for a better exchange of information between central authorities here and overseas; and whereas the previous legislation had a lacuna that left out countries except they were in the Commonwealth, the Bill now applies to all countries, so effectively that gap has been closed.

With respect to the criticisms of Police overreach, it was stated that in Clause 23. it was standardised and on the question of warrants, it had to be done by a Gazetted Officer appearing before a judge or magistrate and not simply a police officer.

18. Hon. Ms. Marsha Caddle – Minister of Industry, Innovation, Science and Technology

(Minister Caddle appeared before the Committee on invitation.)

She stated "*We have received feedback from those who on one hand are extremely passionate about wanting their data protected and those who question the very provisions of the Bill that are specifically designed and drafted to protect people's data. That in essence is the balance that must be struck."*

The Minister goes on:

> *I say that to suggest that we cannot determine that we want to fully experience and enjoy all the benefits of technology and living and working and having our being in an online environment and then pretend that there are not risks and safeguards that must be attached.*
>
> *I have to highlight that data and technology are the new global currency and that they are also at once the new global nuclear weapon. I do not exaggerate the scope for harm in the area of data and technology: where there are no borders; where action is often invisible, the scope must be taken in its full perspective.*
>
> *It is our estimation and it is the experience of many people, that these matters begin to trespass and in fact trespass wholly on the area of criminal harm and damage. Anyone who has anything to say in any circumstance that may cause a nuisance, irritation or that we might like it, is liable to criminal proceedings under this legislation.*
>
> *There must be intentionality behind the act in order for it to stand up to the type of prosecution the Bill contemplates. There is also the evidentiary standard on the part of the prosecution. The evidentiary standard the prosecutor must meet is not just the balance of probabilities. It has to be beyond reasonable doubt. The standard for the defence is on a balance of probabilities.*

The Minister rejected the claim that the Convention on which this legislation is framed is not the best and that there is a UN treaty that is superior to the Budapest convention.

Ethical hacking - someone gains unauthorised access to your data or systems for the purpose of proving vulnerability.

Unauthorised access - Notion that the provision for cyber terrorism is not broad enough.

Clause 26. allows the state.

Clause 28. refers exactly to what it states; that as preservation of data in the manner and format in which it is stored for the purpose of criminal proceedings.

The comment is that in the legislation, there is no discussion of the conditions and safeguards for adequate protection of liberties when collecting and storing data in criminal proceedings including chain of custody. Chain of custody does not enter here because nothing is moving, there is no chain.

All this is saying is if, for example, there is data that is likely to be the subject of criminal proceedings and is being held in the system of a telecommunications company; or in somebody's computer or flash drive, all that is being asked is that the data not be destroyed. There are some companies that data is destroyed after certain periods of time. The request for data to be

preserved means that the time period is not applicable. In our case the warrant is being requested to preserve the data.

The reintroduction of criminal libel with the Cybercrime Bill, 2024.

Minister Caddle stated,

> *The importation of criminal libel into the Cybercrime Bill was to protect people. Civil defamation required persons to have considerable resources to be able to defend themselves because some defamations can be so egregious, and that the scale of damage and injury so great merited it being elevated to the realm of the criminal.*

There are some Barbadians who are aggrieved by some of these actions, they cannot pursue litigation or take any civil action because they simply do not have the resources.

Clause 19.(3) of the Bill purported to create a replacement for criminal libel but sought in its framing to protect freedom of speech by giving the person the right to put forward any of the defences in Clause 19.(3).

These defences matter. So, if a person was charged under Clause 19.(5) and he can prove that he was speaking the truth, he will have a cast iron defence of truth. Truth is the ultimate defence. The aim to protect freedom of speech in the content of criminal libel by the defence is listed at 19.(5).

At Clause 19.(3) it has to be the intentional use of the computer to disseminate information that is false.

The Minister turned her attention to **Clauses 19. and 20**. "**Malicious communication + cyber bullying"**

The Minister stated and is quoted:

> *I think that we have to be tight, precise and clear in our meaning so that if these matters do reach the judicial system, that that system and that process also has clarity and that we can know that prosecutions are likely to succeed if they reach that point. It is for that reason that I think that to the extent that we can remove anything that may be framed or considered vague: that we should do so.*

The Minister proposed an amendment to Clause 19.(3) by deleting the words "*not caring whether they are true or false*" and substitute the words "**that are false**" and "**causes or is likely to cause a person humiliation, embarrassment or reputational injury is guilty of an offence**".

The Minister suggested also the deletions of the words "*ridicule and contempt*". The words ridicule and contempt are deleted.

Clause 20.

Paragraph (b) to be rewritten as follows:

"**for the purpose of causing danger, embarrassment, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress to that person."**

The words "*annoyance, inconvenience, obstruction and insult*" be deleted.

19. The Committee began its deliberations on the following written submissions. Of those presentations which the Committee chose to examine, the comments are cited here:

- **Barbados Bar Association (BAR).**

It was agreed that some of the suggestions of the BAR have merit. Senator Nicholls however stated that the view of the BAR on the unconstitutionality of the Cybercrime Bill 2024 is a misreading of the law in *Hinds v. R.* There was agreement that there was no need to hear orally from the BAR or The Barbados Bankers Association because of the degree of clarity of their submissions.

The Committee discussed the suggestion by the BAR that some of the fines should be lowered. It was agreed that the Court will make a determination as to whether to give the maximum penalty or any penalty in that range and therefore to lower the maximum narrows the scope of culpability. Senator Nurse queried how the determination of the fines are established. The Committee also discussed the suggestion that the Bill should have Regulations to govern enforcement.

- **Barbados Association of Journalist and Media Workers (BARJAM).**

The Chairman noted that the submission by BARJAM commented on the rate of fines in some cases. He stated that since the Minister made concessions to Clauses 19. and 20. that there is no need to address them at this stage. The Chairman acknowledged the request from BARJAM for the 'Freedom of Information' legislation for the press but stated that it was not in the remit of this Committee. However, it can be discussed further in deliberations.

- **The Barbados Police Service (TBPS).**

The Committee noted that they did not raise any issues but just provided commentary on Clauses 19. and 20. of the Bill.

- **The Barbados Bankers Association (TBBA).**

The Chairman noted that the TBBA focused on where actions were taken without authority and recommended a definition of "without authority". He proposed to seek the guidance of

the Office of Chief Parliamentary Counsel who was currently absent. He also noted that the TBBA also raised concerns that some of the Clauses were found to be too broad.

- **Barbados Consumer Empowerment Network (BCEN)**

The Chairman noted that it was the opinion of this submission that there was not enough consumer protection. He believed that this observation did not have merit as regards this particular Bill as opposed to other possible legislation.

- **Mr. Niel Harper, Cyber Security Expert**

The Chairman drew the Committee's attention to Mr Harper's submission in which he indicated that Clause 5. 'Modification of Programme or data" uses outdated language, that the Clause is unnecessary and that the focus should be on someone who intentionally and without authority causes harm. Senator Nicholls queried what is the legislative intent.

Ms Drakes informed the Committee that Clause 5. is the existing law. She further clarified that Section 3 subsections (3), (4) and (5) of the *Computer Misuse* Act, Cap. 124 is incorporated into this Clause, redrafted using in a different format. She also noted that the draft Bill was created in connection with the Council of Europe and that it does not run afoul of the Budapest Convention. She stated that the Budapest Convention does not identify harm or the effect, as a consequence of the offence but that the person intentionally and without authority committed the offence.

The Committee also noted the opinion of Mr Harper which stated that Clauses 5. to 7. seeks to criminalise modern uses of software and data processing. This was also refuted by Ms Drakes as she stated it applies only if a person does not have the requisite permission or authority.

The Chairman raised the query highlighted in some of the submissions of the omission of the word 'recklessly' from some clauses but included in some. Ms Drakes noted that this was mostly a policy decision.

In relation to Mr Harper's comments on Clause 8., Ms. Drakes informed the Committee that the text of the clause is aligned with the Budapest Convention. The Committee determined that his argument was not enough to lower the bar on the intent of the Bill.

The Committee in its discussion of Mr. Harper's comment on Clause 9. considered a suggestion from Senator Nicholls to broaden the scope to include the words "knowledge, permission and consent". The Committee agreed to amend the Bill to include a definition of the term "without authority" in Clause 2.(5).

In relation to Clause 11., the Committee considered the argument by Mr Harper that this is not treated to in the other conventions. Ms. Drakes informed that that clause is currently in the *Computer Misuse* Act, 2005 and that the disclosure must be done intentionally or recklessly and without authority.

- **Mr. Steven Williams, Principal Consultant, Data Privacy and Managements Advisory Services**

The Committee considered two of the issues raised by Mr. Williams.

(1) That the Bill needs Regulations to which Ms. Drakes responded and informed the Committee that Clause 30. of the Cybercrime Bill, 2024 "provides that the Minister may make Regulations generally for the purpose of given effect to this Act." She noted that it is for the piloting Ministry to provide the policy to Chief Parliamentary Counsel (CPC) who will then draft the Regulations; and

(2) The issue of sharing passwords with a third party could lead to a penalty under the Act. The Committee determined that they did not share the view.

- **Mr Anthony Green, General Manager, STARCOM Network**

The Committee agreed that most of Mr. Green's presentation was geared toward freedom of information legislation and that he also spoke in relation to Clause 5. which prohibits illegal interception of data. They further noted his opinion that there should be an exception for journalist and media professionals if the publication is in the public interest. Ms. Drakes explained that there is no criminal offence or penalty for receiving or publishing. The Committee agreed that Ms. Drakes should draft a 'public interest' defence, not just for journalists but for any person acting in the public interest, for the consideration of the Committee.

- **Ms. Janine Butcher, Customer Service Representative**

The Chairman highlighted that her concern was the need to protect whistleblowers who may want to disclose information in the interest of the public and it was agreed that the Committee had already determined the defence of "public interest".

- **Mr. Timon Howard**

The Chairman noted that Mr Howard spoke to the fact that licence should be given for artistic commentary and that it should not attract criminal sanction. The Chairman again queried whether the 'public interest' defence did not apply here. Senator Nicholls suggested that that protection of the artistic commentary should be done at the policy level with the use of prosecutorial guidelines.

- **Mr. Steven Williams**

In conclusion, the Chairman noted that Mr. Williams was generally in favour of the Bill as drafted. The Committee further noted the suggestion by Mr. Williams that critical infrastructure service provisions currently in Clause 12 be placed in Regulations for easier amendment. The Chair proposed that the list of 'critical infrastructure services' be expanded and that the committee would consider that extended list at a later meeting.

20. The Committee consulted the following documents attached hereto and marked "**D1 – D7".**

- **Computer Misuse and Cybercrime Act, Virgin Islands, No. 9 of 2014**
- **Computer Misuse and Cybercrime (Amendment) Act, Virgin Islands, No. 9 of 2019**
- **Cybercrime Act 2018, Guyana**
- **The Cybercrimes Act, Jamaica**
- **Cybercrime Act, 2020, Belize**
- **Guidelines for Prosecuting Cases Involving Malicious Communications: Section 9 of the Cybercrimes Act of Jamaica, 2015**
- **Comparative Table of penalties in Guyana, Jamaica and Barbados legislation presented by Sir David Simmons, KA, B.C.H., S.C.**

21. A. EXAMINATION OF THE CYBERCRIME BILL, 2024

The Committee after deliberations proposed the following amendments to the Bill.

OBJECTS AND REASONS

Long Title

The Committee agreed that the Long Title should remain as stated.

PART I – Preliminary

Short title
Clause 1

The Short title shall remain as stated.

Interpretation
Clause 2. (1)

The Committee agreed to include a definition of "cyber bullying" which reads as follows:

"*cyber bullying*" means the behaviour or conduct referred to at section 20;

The Committee agreed to include a definition of "without authority" because it has been used frequently throughout the provision to the Bill which reads as follows:

"*without authority'* means without right, consent, permission, authorization or in excess of authorization".

Application
Clause 3.

Remains as is.

Illegal access
Clause 4.

Remains as is.

Modification of programme or data
Clause 5.

Remains as is.

Interfering with programme or data
Clause 6.

Remains as is.

Interfering with computer system
Clause 7.

Remains as is.

Illegal interception of data
Clause 8.

Remains as is.

Misuse of devices

Clause 9.

Remains as is.

Access with intent to committee further offence
Clause 10.

Remains as is.

Disclosure of access code
Clause 11.

Remains as is.

Critical information infrastructure system
Clause 12.

Remains as is.

Receiving or giving access to computer programme or data
Clause 13.

Clause 13. (2) *(b)* was amended by deleting the word "and" and substituting the word "**or**" therefor.

Computer-related forgery
Clause 14.

Remains as is.

Computer-related fraud
Clause 15.

Remains as is.

Child pornography
Clause 16.

Remains as is.

Child grooming
Clause 17.

Remains as is.

Online child sexual abuse
Clause 18.

Remains as is.

Malicious communication
Clause 19.

Clause 19.(1)*(b)*(ii) the words '*on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both*' were deleted and substituted with the words:

" **(A) on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or**

(B) on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both."

Clause 19.(2)*(b)* the words '*on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both*' were deleted and substituted with the words:

" **(i) on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or**

(ii) on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both."

Clause 19.(3) The words *'not caring whether they are true or false'* be deleted and substituted with the words, "**that are false"***;* the words '*ridicule', 'contempt'* and '*embarrassment'* were deleted*;* and substituted with the words '*humiliation or injury'* and the words '*on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both*' were deleted and substituted with the words:

"(a) on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or

(b) on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both."

Clause 19. (4) The words '*subsection (1)'* was deleted and substituted with the words **"this section",**

Clause 19.(4) *(b)* the word **"reputation"** was inserted before the word *'business".*

Cyber bulling
Clause 20.

Clause 20.(1) the rubrics '*(a)'* and '*(b)'* were deleted to make one paragraph.

The words "*annoyance', 'inconvenience', 'obstruction', 'embarrassment', and 'insult'* were deleted and the words '*on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both*' were deleted and substituted with the words:

"(a) **on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or**

(b) **on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both."**

Cyber terrorism
Clause 21.

Remains as is.

Aiding or abetting
Clause 22.

Remains as is.

PART III
INVESTIGATION AND ENFORCEMENT

Search and seizure
Clause 23.

Clause 23.(1) The words **'Judge or'** was inserted before the word *'magistrate'* at line 5.

Clause 23.(2)*(a)*. The words, *"***or contains evidence***"* was inserted before the words *'that an offence has been or is about to be committed;'*

Assisting a police officer
Clauses 24.

Remains as is.

Record of seized data to be provided to the owner
Clause 25.

Remains as is.

Production of data for criminal proceedings
Clause 26.

Remains as is.

Expedited preservation and partial disclosure of traffic data
Clause 27.

Remains as is.

Preservation of data for criminal proceedings
Clause 28.

Remains as is.

Order for payment or compensation
Clause 29.

Remains as is.

Regulations
Clause 30.

Remains as is.

Consequential amendments
Clause 31.

Remains as is.

Repeal
Clause 32.

Remains as is.

Commencement
Clause 33.

Remains as is.

22. EXAMINATION OF THE MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024.

There were no suggested amendments to the Bill as drafted.

23. CONCLUSION

Having given due consideration to the various submissions – written and oral; and after interaction with those presenters along with the many robust discussions and with the benefit of guidance by Ms. Rhea Drakes, Parliamentary Counsel of the Office of the Chief Parliamentary Counsel, the Committee agreed to the amendments as shown and are reflected in the redrafted Cybercrime Bill, 2024 appended hereto and marked **"E1"**

Transcripts of all the meetings are appended hereto and marked **"F1" – "F7".**

ACKNOWLEDGEMENTS

The Committee wishes to acknowledge and thank all those organisations and persons who took the time and effort to submit written submissions. An expression of gratitude is extended to all those who were willing to make oral presentations before the Committee stimulating numerous questions and worthwhile discussions.

Though the Committee may not have agreed with all the concerns raised or with all the suggestions and the recommendations put forward, it is forever grateful for the different perspectives and views shared which valuably assisted it in making the relevant amendments reflecting greater transparency and accountability.

The Committee expresses its sincere thanks and appreciation to Sir David Simmons, KA., B.C.H., S.C., Chairman of the Law Reform Commission for his contribution to the Committee's work. An immense amount of gratitude is also expressed to Ms. Rhea Drakes, Parliamentary Counsel (CPC), for her tremendous assistance in enabling the Committee to accomplish its work in a satisfactory manner. The Committee further extends gratitude to the Office of the Clerk and the staff of Parliament for their diligence and commitment in expediting the work of the Committee.

Approved by the Members of the Committee: -

Mr. Edmund G. Hinkson, S.C., M.P. *(Chairman)* _____

Dr. Romel O. Springer, J.P., M.P. *(Deputy Chairman)* _____

Mr. Peter R. Phillips, J.P., M.P. _____

Mr. Ralph A. Thorne, K.C., M.P. _____

Senator Gregory P. B. Nicholls _____

Senator Ryan O. Walters _____

Senator the Hon. Lindell E. Nurse _____

Dated this 8th day of August , 2024.

MINUTES

PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2022 - 2027)

JOINT SELECT COMMITTEE (STANDING)
ON GOVERNANCE AND POLICY MATTERS

Minutes of the First meeting of the Joint Select Committee (Standing) on Governance and Policy Matters and its Preliminary meeting on the review and examination of the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024, held in the Senate Chamber, Parliament Buildings, Trafalgar Street, Bridgetown, St. Michael on Monday, April 8th, 2024 at 2:00 p.m.

PRESENT WERE:

Mr. Edmund G. Hinkson, S.C., M.P.
Mr. Peter R. Phillips, J.P., M.P.
Dr. Romel O. Springer, J.P., M.P.
Senator Gregory P. B. Nicholls
Senator the Hon. Lindell E. Nurse

ABSENT:

Mr. Ralph A. Thorne, K.C., M.P. (Leader of the Opposition)
Senator Ryan O. Walters

IN ATTENDANCE WERE:

Mr Pedro Eastmond, *Clerk of Parliament*
Ms. Beverley S. Gibbons, *Deputy Clerk of Parliament*
Miss Suzanne Hamblin, *(Journal Department)*

Excuses were made on behalf of Mr. Ralph A. Thorne, K.C., M.P. (Leader of the Opposition) and Senator Ryan O. Walters

Call to Order

The Meeting was called to order by the Clerk of Parliament, Mr Pedro Eastmond at 2:10 p.m.

Item 1: Appointment of Chairman and Deputy Chairman

The Clerk of Parliament invited a nomination for the appointment of a Chairman. On the motion of Senator Gregory P. B. Nicholls, seconded by Dr. Romel O. Springer, Mr. Edmund G. Hinkson, was nominated. A vote being taken, Mr Hinkson was appointed the Chairman of the Joint Select Committee (Standing) on Governance and Policy Matters.

Mr Edmund G. Hinkson assumed the Chair and thanked members for the appointment.

The Chairman invited nominations for the appointment of a Deputy Chairman.

On the motion of Senator Gregory P. B. Nicholls seconded by Senator the Hon. Lindell E. Nurse, Dr. Romel O. Springer was nominated. A vote being taken, Dr. Springer was appointed Deputy Chairman of the Joint Select Committee (Standing) on Governance and Policy Matters.

Item 1: Execution of the Terms of Reference

The Chairman invited members to examine the draft Terms of Reference dated 2024-04-08 that were prepared by him and circulated by the Office of Parliament.

The Committee engaged in discussion on the draft terms of reference and agreed that the following would constitute the Terms of Reference on the Bills:

1. To enquire into and determine whether the Cybercrime Bill as drafted fulfils the expressed purposes to ensure compliance with the International Conventions, global standards and best practices to counter cybercrime and to ensure international cooperation in the combatting of cybercrime.

2. To examine whether the Cybercrime Bill as drafted curtails the citizens' fundamental rights to freedom of expression as against the protection of the reputation, rights and freedoms of other persons or their private lives.

3. To examine whether the Cybercrime Bill as drafted provides the necessary checks and balances, safeguards and independent oversight to protect citizens' human rights, liberties and privacy rights from potential abuses, including from expansive law enforcement powers in order to prevent miscarriages of justice.

4. To examine whether the Cybercrime Bill as drafted provides adequate protection to all of the specific categories of persons who may potentially be vulnerable to cybercrime.

5. To examine whether any of the provisions of the Cybercrime Bill as drafted are vague, overly broad, arbitrary and/or subjective and uncertain in its imposition of liability.

6. To examine whether the penalties imposed in the Cybercrime Bill as drafted are disproportionate and/or unreasonable in any way.

7. To examine whether the Cybercrime Bill as drafted provides adequate protection for whistleblowers who expose cyber-related wrongdoing and, if not, whether such protection is provided in any other legislation.

8. To consider whether the Cybercrime Bill as drafted could impede innovation in the technology sector and discourage investment and research in digital infrastructure.

9. To consider whether the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024 as drafted provides adequately for mutual international assistance in matters relating to computer-related crimes and for related matters.

10. To make recommended changes, if deemed necessary, to the Bills as drafted for further consideration by the Chief Parliamentary Counsel.

Item 3: Scope of Works

The Clerk of Parliament informed the members of the Committee that the Chief Parliamentary Counsel should form part of the Committee and attend all meetings to give guidance on the legislation.

The Committee agreed that specific organisations, interest groups and individuals should be invited to present either oral or written presentations.

The Committee determined that the following would be specially invited to make submissions:

- Democratic Labour Party
- Barbados Labour Party

- Rev Bishop Joseph Atherley
- Sir David Simmons, K.A., Chairman of the Law Reform Commission
- Mr Niel Harper
- Ms Stephanie Chase
- Mr Kammie Holder
- Mr Peter Thompson
- Ms Marcia Weekes
- Mr Steven Williams
- Mr Kemar Stuart
- Mr Anthony Clerk, Barbados Bankers Association
- Starcom Network Inc.
- Barbados Bar Association
- Commissioner of Police
- Barbados Today Newspaper
- Caribbean Broadcasting Corporation
- Nation Publishing Co. Ltd.
- Barbados Association of Journalists & Media Workers (BARJAM)

The letters of invitation would be sent out by the Office of the Clerk.

The Committee agreed that the meetings should be in-person. The Chairman queried whether there is a need for Townhall meetings. The decision was taken to consider that, if necessary, at a later date. The Committee also agreed that Zoom would be available to the Committee and that public meetings and oral presentations would be live streamed on the Parliament's website, and Parliament's YouTube Channel and that the link would be shared in the Press Release and on the various platforms.

The Committee agreed that all media houses would be informed of the work of the Committee and invited to the public meetings.

The Committee was reminded of the scheduled reporting of 90 days from the date of reference which was 14th February, 2024.

The Clerk of Parliament indicated that with the recent changes to the composition of the Honourable the Senate the Committee was only fully constituted 2 weeks ago. It was agreed that the Committee would seek an extension to consider its work.

Item 4: Should each Bill be dealt separately or taken together given that the subject matter is linked.

The Chairman proposed and it was agreed, that with regards to the public, oral and written presentations could be on both Bills but that the Committee in its deliberations would consider them separately.

Item 5: Advertisement by the Clerk's office to the public; timelines to submit written submissions and to make oral presentations; timeline for the Committee to finish deliberations and to complete the Report to be laid in the House of Assembly.

The Committee having already agreed that given the late start of the work of the committee that it would seek an extension to complete its work and determined that the public should be given two (2) weeks from the date of publication of the Press Release to submit their presentations. Senator Gregory P. B. Nicholls made the suggestion that the submissions should be in writing with the Committee having the option of asking individuals to appear in person if the Committee so desires.

The Clerk of Parliament read a Press Release used by another Joint Select Committee (Standing) and it was agreed that with modifications this Committee's Press Release could follow in a similar vein. It was agreed that the Press Release should appear in both the Nation Newspaper and Barbados Today E-paper and published by weekend; and that it be sent to the Government Information Service (GIS) for dissemination to the other media houses.

Item 6: Any Other Business

The Chairman requested that the following research documents be made available to Committee Members before the next meeting;

- United Nations Conventions

- Other Cybercrime Legislation: Jamaica, Guyana
- Budapest Convention
- Information from European Union Meeting held in Barbados- October 2023
- Debates of the House of Assembly on the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024.
- Any other pertinent information.

The Committee agreed that the next meeting be held on Thursday 18th April, 2024 and that the Office of the Chief Parliamentary Counsel and Sir David Simmons, KA be invited to the meeting.

ADJOURNMENT

There being no further business, on the motion of Senator Gregory P. B. Nicholls seconded by Mr. Peter R. Phillips the meeting was adjourned to Thursday, April 18th, 2023 at 2:00 p.m.

The Chairman adjourned the meeting accordingly at 3:58 p.m.

Nedra. S. Sandiford

Clerk of Parliament

Confirmed this 22nd day of April 2024.

Edmund S. Hinkson

Chairman

PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2022 - 2027)

JOINT SELECT COMMITTEE (STANDING)
ON GOVERNANCE AND POLICY MATTERS

Minutes of the Second meeting of the Joint Select Committee (Standing) on Governance and Policy Matters on the review and examination of the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024, held in the Senate Chamber, Parliament Buildings, Trafalgar Street, Bridgetown, St. Michael on Monday, April 22nd, 2024 at 2:00 p.m.

PRESENT WERE:

Mr. Edmund G. Hinkson, S.C., M.P. **(Chairman)**
Dr. Romel O. Springer, J.P., M.P.
Mr. Ralph A. Thorne, K.C., M.P.
Senator Gregory P. B. Nicholls
Senator the Hon. Lindell E. Nurse
Senator Ryan O. Walters

ABSENT:

Mr. Peter R. Phillips, J.P., M.P. *(Excused)*

IN ATTENDANCE WERE:

Mr Pedro Eastmond, *Clerk of Parliament*
Ms. Beverley S. Gibbons, *Deputy Clerk of Parliament*
Mr Nigel Jones, *Deputy Clerk of Parliament*
Miss Suzanne Hamblin, *(Journal Department of Parliament)*
Sir David Simmons, KA., *Chairman of the Law Reform Commission*
Ms Rhea Drakes, *Parliamentary Counsel, Office of the Chief Parliamentary Counsel*

Item 1: Call to Order and Welcome

The Meeting was called to order by the Chairman at 2:15 p.m.

The Chairman welcomed Sir David Simmons, K.A., Chairman of the Law Reform Commission who was invited to give his input and technical support on the Cybercrime Bill, 2024.

He also welcomed Mr Ralph A. Thorne, Leader of the Opposition and other members of the Committee, the representative of the Chief Parliamentary Counsel and the staff of the Parliament.

Item 2: Minutes of the Preliminary Meeting held on Monday, 8th April, 2024

On the motion of Senator the Hon. Lindell E. Nurse seconded by Dr. Romel O. Springer the minutes were confirmed with amendments. The amendments at page 4 related to the names of the persons/organisations that were to be sent invitations but were omitted.

Item 3: Matter Arising

The Chairman noted that the Committee had already received submissions from Niel Harper and Steven Williams. The Committee was also informed of the request from Niel Harper that, due to his being out of the jurisdiction, he would like to make his presentation over the Zoom platform.

Item 4: Consideration of the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024.

(i) **Technical Support** - Sir David Simmons K.A., Chairman Law Reform Commission
- Chief Parliamentary Counsel

Sir David Simmons introduced Ms Rhea Drakes from the Chief Parliamentary Counsel's Office who was the officer with responsibility for drafting the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024.

Sir David gave an overview of the Cybercrime Bill and its purpose and in his presentation commented and explained several aspects of the Bill. He also gave an analysis of the criticisms of the Bill. He further gave a summary of the Law Reform Commission's position on the Bill and commented

on the Terms of Reference of the Committee. Sir David entertained questions and queries from members of the Committee. (*Transcript attached*)

Sir David referred to a table of comparative analysis of legislation and the penalties in similar legislation from several jurisdictions and agreed to provide a copy for the benefit of members of the committee.

Mr Chairman thanked Sir David Simmons for his presentation.

Item 6: Any Other Business

The Committee agreed that the next meeting would be held on Monday 6th May, 2024 and that it would hear oral presentations from the two persons who had submitted presentations namely Niel Harper and Steven Williams. The Committee further agreed that Mr Harper will present via Zoom.

The Clerk of Parliament referred to the email sent by Senator Tricia Watson in relation to the press release. She indicated that the Committee should allow the diaspora to appear using the Zoom platform and that notices of subsequent meetings should appear in both the audio and print media. The Committee agreed.

ADJOURNMENT

There being no further business, on the motion of Senator the Hon. Lindell E. Nurse seconded by Senator Ryan O. Walters the meeting was adjourned to Monday, May 6th, 2024 at 2:00 p.m.

The Chairman adjourned the meeting accordingly at 5:12 p.m.

Clerk of Parliament

Confirmed this 6th day of May 2024.

Edmund F. Hinlyson

Chairman

PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2022 - 2027)

JOINT SELECT COMMITTEE (STANDING)
ON GOVERNANCE AND POLICY MATTERS

Minutes of the Third meeting of the Joint Select Committee (Standing) on Governance and Policy Matters on the review and examination of the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024, held in the Senate Chamber, Parliament Buildings, Trafalgar Street, Bridgetown, St. Michael on Monday, May 6th, 2024 at 2:00 p.m.

PRESENT WERE:

Mr. Edmund G. Hinkson, S.C., M.P. **(Chairman)**
Mr. Peter R. Phillips, J.P., M.P.
Dr. Romel O. Springer, J.P., M.P.
Mr. Ralph A. Thorne, K.C., M.P.
Senator Gregory P. B. Nicholls
Senator the Hon. Lindell E. Nurse
Senator Ryan O. Walters

IN ATTENDANCE WERE:

Mr Pedro Eastmond, *Clerk of Parliament*
Miss Suzanne Hamblin, *(Journal Department of Parliament)*

ABSENT:

Ms. Beverley S. Gibbons, *Deputy Clerk of Parliament*
Ms Rhea Drakes, *Parliamentary Counsel, Office of the Chief Parliamentary Counsel (Excused)*

Item 1: Call to Order and Welcome

The Meeting was called to order by the Chairman at 2:15 p.m. who welcomed all present.

Item 2: Minutes of the Second Meeting held on Monday, 22nd April, 2024

Deferred.

Item 3: Matter Arising

Deferred.

Item 4: Oral Presentations (*Transcript attached*)

Mr Niel Harper, Cyber Security Expert

Mr Steven Williams, Principal Consultant, Data Privacy and Management Advisory Services

Mr Anthony Green, General Manager – Starcom Network Inc

Mr Kemar Stuart

His Excellency Rev Dr. Ferdinand Nicholls, ORDM

It was agreed by the Committee that presenters would be allowed a maximum of 10 minutes for their submissions principally to expand on points made in their written submissions and thereafter the members of the committee would be permitted to ask questions.

(i) Mr. Niel Harper, Cyber Security Expert

Mr Niel Harper gave his presentation via the Zoom platform.

Mr Harper began by referencing the countries where there were abuses of Cybercrime Law and gave instances of such abuse. He stated that his major concern was that the Bill as drafted could result in the abuse of the law from the perspective of suppression of public discourse in terms of violation of human rights.

He was concerned that Barbados does not have trained court officials or a specialized court for example, the UK has the King's Bench division on Technology, which has specialist judges who are

known as Masters and who have special training to address and adjudicate on these type of matters to ensure that innocent or well-meaning persons are not imprisoned.

He raised an issue with Part II Clause 5. of the Bill - 'Modification of programme or data.' He stated that this section is misaligned with the Budapest Convention, Commonwealth Model Law on Cybercrime, the Malabo Convention, and other cybercrime model laws which do not mention "modification of programmes or data" in terms of criminality and that the section also uses outdated language and criminalises several modern, productive use cases for software and data processing (e.g., AI, free and open-source software, open data policies, creative commons, data mining, etc.). He continued that this section should be removed as it can be addressed by Clause 6 - Interfering with programme or data and which itself should be changed to 'Interfering with data' for better alignment with the Budapest Convention. Even so this clause itself uses outdated language and should really focus on someone who intentionally, without authority causes harm. He stated that if something is temporary and does not cause harm it should not be a crime and criminalizing minor acts, especially acts that do no harm is unnecessary.

As regards to Part II Clause 7. 'Interfering with computer system', he said that the same principle applied in that it does not really address the true criminality which is really focused on intention, without authority and seriously hindering the functioning of a computer.

As regards to Part II Clause 8. 'Illegal interception of data', he stated that this Clause indicated a lack of understanding of modern computer systems and data management.

As relates to Part II Clause 9. 'Misuse of devices', he referenced the Budapest Convention which says that misuse of devices, illegal access, interfering with a system, all of these should not be interpreted as imposing criminality and not for the purpose of committing an offence where it is authorised testing or protection of a computer system. He noted that where there is legitimate use to protect a computer system to ensure a computer system is robust and resilient, these type of laws should not be used to criminalize those practices.

As regards to Part II Clause 12. 'Critical information infrastructure system'- he said his concern with this section is that it is unnecessary for the Cybercrime Bill since the offences and penalties are already addressed in multiple different sections of the Bill. He suggested creating separate legislation that focuses on critical infrastructure protection.

Part II Clause 19. 'Malicious communications' - He indicated that the Budapest Convention and other model laws do not address malicious communication and that trying to include it in the Cybercrime Bill is very problematic because the European Court of Human Rights, the United Nations, several

human rights organizations, as well as international intergovernmental bodies maintain that criminal defamation laws are unjustifiable affronts to human rights and that several progressive nations have actually removed criminal defamation laws from their books.

Part II Clause 20 'Cyber bullying' - He opined that in relation to this section, that adults are supposed to be resistant to hurtful words and that across progressive nations, cyber bullying laws focus on schools, children and adolescents and when they do focus on adults they are particularly restricted to violent acts, sexual abuse and harassment.

Part III, Clause 23. 'Search and seizure' - He added that in his opinion Barbados has a problem with capacity building in that we do not have a national strategic cybercrime capacity building approach for training the law enforcement, prosecutors, magistrates and judges in terms of making sure that they have continuous development and that they understand existing and emerging technology; how those technologies interact with the law, and to ensure that they have the right knowledge and skillset that they can actually administer these types of cases when they do come in front of them.

Mr Harper responded to the Chairman and other members in response to queries on matters on which he might have been misunderstood.

(ii) Mr. Steven Williams, Principal Consultant, Data Privacy and Management Advisory Services

Mr Williams thanked the Committee for it invitation to appear before it. He also expressed thanks to Sir David Simmons, Chairman of the Law Review Commission for selecting him as the IT Consultant on the Cybercrime Bill.

He began his presentation recounting that approximately 12 years ago he was the victim of malicious defamation by a perpetrator outside of the jurisdiction and he had no recourse due to the limited scope of the *Computer Misuse* Act, 2005. He also informed that as a former member of the Board of Directors of the Transport Authority, he witnessed fraudulent documents submitted to the Board falsely alleging to have been authorised by the Chairman of the Board.

He noted that the Cybercrime Bill gives the police a strengthened tool to pursue individuals who aim to deceive and exploit the system using computer related fraud as it empowers them to investigate and prosecute those who manipulate digital information. He stated that the Bill establishes a framework that tackles the threat of cybercrime itself which includes child exploitation and misuse of digital devices.

He however acknowledged the concerns that have arisen from various stakeholders and sought to give his perspective on some of those concerns:–

Illegal access provisions:- He noted that while it is not a custom for cyber professionals to illegally break into a network or computer system without proper clearance, it is up to the judiciary to determine the criminality i.e. malicious intent or unauthorised action. As regards to activist, it was the judiciary's duty to determine the difference between malicious intent and those actions which though well intended could cause harm;

Critical Information infrastructure systems (CIS): - He opined that it was crucial to promptly publish complimentary regulations to ensure regular updates to the CIS listings that incorporates evolving technology with AI;

Malicious Communication: - He posited that there should be a careful balance to ensure that the judiciary discerns between malicious intent and legitimate public discourse so that it protects victims from unwarranted attacks from those who intentionally and recklessly use computer systems to intimidate, threaten or defame, while appearing not to stifle free speech;

Disclosure of access codes: - He reflected on this aspect of the Bill and posited that at this section it may be more appropriate for corporate disclosure of passwords rather than domestic sharing which could be seen as a civil matter noting that everyday password sharing activity could be discerned harmful activity. He left that to the committee to decide;

He concluded his presentation by giving the committee three (3) point to consider – Intent; Symbiotic Regulations and Password Sharing.

Senator Gregory Nicholls asked Mr Williams to elaborate on his position regarding his proposal for regulations and the governing agency to issue same and its capacity so to do to which he replied that the regulations should determine what the qualifications would look like in terms of the critical infrastructure list. He added that in addition to regulations that there would be a need for an Information Technology Authority to assist the Ministry. When further questioned as to how this environment could be regulated he responded that there would be a need for additional resources for role playing.

When questioned by Mr Ralph Thorne on how he saw his purpose before the committee; whether supporting or opposing the Bill given his role in its drafting, Mr Williams responded that while he supported the Bill he was of the opinion that it was not a perfect piece of legislation, hence the rationale for being before the Committee. He further elaborated that it was a significant improvement on the *Computer Misuse* Act.

The Chairman queried of Mr Williams his opinion of sections 12 – 23 and whether as drafted they infringed unduly and unreasonably on the constitutional right of freedom of expression. His response was that he did not think so and that the Bill only seeks to punish for intent to harm someone or their character using a device.

Dr Romel Springer questioned Mr Williams about his reference in his submission to section 11 where he suggested that there should be a category that spoke to commercial versus domestic misuse of access codes and asked him to expand noting that the Bill speaks to "recklessly, intentionally and unlawful gain". Mr Williams reiterated that in his opinion there was a need for regulations to take care of the nuances.

Mr Thorne queried of Mr Williams his opinion as to whether the major focus of the Bill is the pursuit of persons overseas who are offensive to persons in Barbados and who are otherwise difficult to capture by a defamation lawsuit. Mr Williams responded that he was not aware that any specific area had more attention than others but that when the *Computer Misuse* Act was drafted there was no social media as it currently exist the intention was to draft an updated Bill that covers greater areas and the Bill was for the protection of all persons whether in Barbados or abroad as long as there is a jurisdictional relationship.

Mr Chairman questioned Mr Williams about his statement in his written submission that the definition of cyberterrorism should be expanded. He responded than on reflection he would withdraw that statement with the view that it can be covered in the anti-terrorism legislation, again looking forward to any nuances in the Bill being covered by Regulations.

Mr Chairman asked Mr Williams to comment on whether he would eliminate or advise to eliminate sub-clause 11. (1) or 11 (2) of the Bill and which one since they may be interpreted as repeating themselves. He replied that he was not sure what would be the judiciary's interpretation of them if left in. He gave his thoughts on both cases but he opined that there was a nuance thereon which he did not see as a non-lawyer.

Additionally, Mr Chairman sought from Mr Williams his opinion on the intimidation aspect of the legislation in clause 19 (1) (a) and drew a comparison to a similar clause in the Guyana legislation. Mr Chairman stated that it was criticised by some as to intimidating a person and intentionally or recklessly through a computer system and asked Mr Williams if he would recommend a change. Mr Williams opined that it should be left in while noting that there can be no separation between politics and everyday experiences, and further that to adopt the Guyana version may weaken the law.

Senator Ryan Walters enquired from Mr Williams as an IT Consultant what would be the specific areas of IT that would have been fed into this Bill. Mr Williams indicated that it would have been of a technical nature, referencing Internet Service Providers and traffic data; how technology might be impacted and how people might impact technology, and how the Bill may affect such. He noted too that it considered the future of technology and the requirement to store data and for how long and what condition it may be in for any particular length of time.

The Chairman thanked Mr Williams for his presentation.

Mr Chairman craved the indulgence of the Committee to and addressed a matter published in the Nation Newspaper on 25th April, 2024 which reported on comments made by Mr Caswell Franklyn.

(iii) Mr Anthony Greene, General Manager , STARCOM Network

Mr Green began his presentation by noting that due to the timelines of the Committee he opted for an oral presentation and that he was not fully prepared to address specifically the content of the Bill but to address the perceptions that have arisen from the debate. He noted that communication is the crux of everything and the introduction of the Cybercrime Bill was the opportune moment to consider how the country communicates not just facilitating designated information but also empowering citizens to actively engage in discussions.

He stressed the importance of not stifling the freedom of the press and expression or the perception thereof. He urged that there need to be a delicate balance between protecting individuals from cyber threats and upholding the principles of transparency and accountability. He cautioned against the perception that the aim of the Bill is restriction of the flow of information or fostering a culture of secrecy but rather approach its implementation with a nuance understanding of the security concerns and democratic principles. He referenced the instance in 2017, the Center for Law and Democracy (CLD) posted on their website concerns about the Cybercrime Bill in Trinidad and Tobago in which there were strong concerns about vague and over broad content; offences which would have prohibited a range of innocuous, normal or even beneficial online activity which still exist.

He said that section 7 'Illegal interception of data' of the Trinidad Bill was deleted but that the Barbados' Cybercrime Bill has a similar clause in section 8. He continued that CLD posting pointed out that the prohibitions were so broad that they create a presumption of criminality leaving for some expressive users the onus to demonstrate that their actions are legitimate which runs contrary to international freedom of expression standards. He opined that the term "justifications" is unduly vague.

He also expressed concern that journalists or media personnel should be allowed to receive and report on information they receive without fear of retaliation as long as they are acting in the interest of the public which is the core work of the media.

He stressed that Barbados lacks what he termed as a very important piece of legislation which would address many of the concerns surrounding the Cybercrime Bill, in that Barbados does not have a Freedom of Information Act or an Access to Information Act. He referenced several Caribbean countries with such or similar legislation and urged that Barbados seriously move towards implementation.

He concluded that the enactment of the Cybercrime Bill presented the opportunity for Barbados to reaffirm its commitment to effective communication practices. He further gave clarity to his thoughts in answers to queries from members of the Committee.

(iv) His Excellency Rev. Dr Ferdinand Nicholls

Reverend Dr Nicholls indicated that his concerns with the legislation were of a broad nature and noted that the voice of the people is the voice of God. His main concern and opposition to the Bill is found in sections 19 to 23 which in his opinion needed to be dramatically amended or removed totally. He was concerned that sections of the Bill are criminalising the Barbados public rather than ensuring the safeguards and conditions identified by the Cybercrime Convention and aspects of the United Nations Charter on Human Rights.

In response to Dr Romel Springer, concerning sections 19 to 23, he responded in particular regarding the definition of the word 'bullying' and the fines attached to the proposed crime of cyberbullying; he felt with regards to the words in section 20 of the Bill and the definition that he as a preacher, delivering a message from the pulpit, could find himself committing a crime. He opined that the Bill uses language that is open to being deemed as vague, overly broad, arbitrary and or subjective and uncertain and expands the potential reach of the law beyond what is necessary or clear.

(v) Mr Kemar Stuart – Non Resident Research Fellow; Caribbean Progresss Studies Institute

Mr Stuart began his presentation by indicating his concern with Part III – Investigation and Enforcement, and posited that words like "insults, humiliation and embarrassment" are very emotive and a person using social media though well intentioned may cause such and find themselves punishable by the Court.

His second point and criticism concerned the extraordinary powers of 'search and seizure' being given to the Police Service and opined that persons would have to be actively monitored by the police for the police to be aware of a crime being committed.

His third point was on the resources of the Police Service to equip them to adequately carry out the requirement of the Bill. Additionally, he questioned the amendment to the Mutual Assistance in Criminal Matters (Amendment) Bill which expands the list of countries that will be added under the information sharing conventions. Mr Stuart also suggested that in the Cybercrime Bill there should be a section which speaks specifically about criticism of public officials rather than the Bill having a list of crimes that would not be considered political crimes. He stated that he thinks that there is an attempt to regulate or overregulate to the point that it has gone pass security and it is an attempt to control the freedom of expression used through social media. His final point dealt with section 25 and the power of the police to confiscate devices.

Item 2 (recommitted) : Minutes of the Second Meeting held on Monday, 22nd April, 2024.

On the. Motion of Senator G. P. B. Nicholls seconded by Mr P. R. Phillips the Minutes of the meeting of Monday 22nd April, 2024 were confirmed.

Item 3. Recommitted: Matters Arising

There were none.

Item 6: Any Other Business

The Chairman stated that the committee had received over 43 submissions and that he had siphoned out around 12 persons to give oral evidence in addition to the four others. There was discussion and it was the determination of Committee to hear an additional 5 persons at the next meeting namely Janine Butcher, Victor Lewis, Heather Cole, Timon Howard and Rosaline Corbin. The Committee also agreed that it would hear from the Minister of Innovation, Science and Technology, Honourable Ms Marsha Caddle, MP at the next meeting. It was further noted that Sir David Simmons, Chairman of the Law Reform Commission would like to reappear before the Committee to finish off the evidence taking.

The Chairman asked and the Committee agreed to accept the submission by the Barbados Police Service despite it being received after the deadline.

ADJOURNMENT

There being no further business, on the motion of Senator G. P. B Nicholls seconded by Mr. P. R Phillips the meeting was adjourned to Monday, May 13th, 2024 at 10:00 a.m.

The Chairman adjourned the meeting accordingly at 6:35 p.m.

Pedro. L Eastmond

Clerk of Parliament

Confirmed this 4th day of July 2024.

Edmund G. Hinkson

Chairman

PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2022 - 2027)

JOINT SELECT COMMITTEE (STANDING)
ON GOVERNANCE AND POLICY MATTERS

Minutes of the Fourth Meeting of the Joint Select Committee (Standing) on the review and examination of the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024, held in the Senate Chamber, Parliament Buildings, Trafalgar Street, Bridgetown, St. Michael on Monday, 13th May, 2024 at 10:00 a.m.

PRESENT WERE:

Mr. Edmund G. Hinkson, S.C., M.P. (**Chairman**)
Dr. Romel O. Springer, J.P., M.P.
Mr. Peter R. Phillips, J.P., M.P.
Mr. Ralph A. Thorne, K.C., M.P.
Senator Gregory P. B. Nicholls
Senator the Hon. Lindell E. Nurse
Senator Ryan O. Walters

IN ATTENDANCE WERE:

Mr Pedro Eastmond, *Clerk of Parliament*
Ms. Beverley S. Gibbons, *Deputy Clerk of Parliament*
Miss Suzanne Hamblin *(Journal Department of Parliament)*
Ms. Rhea Drakes, Parliamentary Counsel *(Office of the Chief Parliamentary Counsel's Office)*

Call to Order and Welcome

The Chairman called the Meeting to order at 10:25 a.m. and welcomed everyone.

Item 2: Minutes of the Third Meeting held on Monday, 6th May, 2024

The Minutes of the Meeting of Monday, 6th May, 2024 were deferred on the motion of Senator Gregory P. B. Nicholls seconded by Mr. Peter R. Phillips.

Item 3: Matters Arising

They were consequentially none.

Item 4: Oral Presentations

The Committee continued with the following oral presentations which were again facilitated by Zoom facilities and lived streamed: -

(i) Ms. Janine Butcher, Customer Service Representative

Ms. Butcher testified virtually *via* Zoom. She proffered her concerns in relation to the Cybercrime Bill, 2024 (CB). She believed that in seeking to protect individual's rights to access their information there should be the utilisation of procedural safeguards. She stated that there was a concern about the potential for abuse of the Bill for political or personal reasons and stressed that the expansive powers given to law enforcement agencies should be balanced carefully to prevent misuse.

She made the following recommendations to the Committee amongst others:

1) With regard to stifling political dissent, safeguards in the law should be implemented to prevent the Bill from being misused to target individuals expressing legitimate political concerns or opinions so as to uphold the principles of free speech;

2) To prevent any biases further safeguards should be utilised to prevent selective enforcement based on political affiliations, personal vendettas or other non-criminal motivations; and

3) To assist in the mitigation of the risk of abuse there is a need to establishing independent oversight bodies separate from law enforcement agencies.

Mr. Chairman pointed out that this final recommendation would just add to more bureaucracy and assured that once the Bill was passed and enacted, that those with responsibility over law enforcement would make the necessary adjustments and operate accordingly.

(ii) Mr. Victor Lewis, retired Police Officer and Educator

Mr. Lewis appeared before the Committee in person and his testimony was based on the CB, 2024. He testified that the Bill seeks to criminalise free speech as set out under "Malicious communications", Clause 19.(1) and this was not in the best interest of the development of Barbados. He was also concerned about "Search and seizure" as provided pursuant to Clause 23.(1), where he cited *'reasonable grounds for suspecting that an offence has been, is being or is about to be committed...'* He felt that the wording was ambiguous. He was reminded by Ms. Rhea Drakes, CPC that this provision was currently the law in Section 23 of the Computer Misuse Act, Cap 124B.

(iii) Ms. Heather Cole, Budget Analyst, New York

Ms. Cole who resides in New York appeared before the Committee *via* Zoom. She submitted that she primarily had three (3) concerns with the CB, 2024. One notable concern was that there was no mention of surveillance and detention within the Bill as it failed to state what happens to a person after the search or prior to the appearance in court and wondered whether Barbados was about to become a police state.

She concluded that the Bill offers no protection from bad actors in the Civil Service or Parliament. She opposed the Bill in its present form because she believed it may have significant changes that would affect our Constitution as it relates to freedom of expression.

In relation to the issue of breaching one's constitutional right to freedom of expression, Mr. Chairman pointed out to her that Clause 19.(5) in the Bill speaks to the defences to a charge on an allegation of a breach of the CB, 2024.

(iv) Mr. David Weekes, Retired

Mr. Weekes who resides overseas testified virtually *via* Zoom. His submission to the Committee was with regard to the CB, 2024. He queried the reliance of certain words contained under "Cyber bullying", Clause 20.(1), *'annoyance'*, *'inconvenience'*, *'embarrassment'*, *'insult'*, *'humiliation'*, *'intimidation'* and *'anxiety'*. He suggested that there was a disingenuous concatenation being relied on because these were delicate words and not criminal acts.

He testified that there were justifiable issues that the Bill addresses, namely illegal and reprehensible acts that require the enactment of the law to protect the rights of citizens, politicians and their friends. He suggested that in our new Republic, the State endorses threats and denies the rights of freedom of expression.

He also suggested that the Bill was equivalent to Thailand's lèse-majesté laws which "forbids the insult of the monarchy", and they have the strictest regulation on free speech in the world. He stated that the CB, 2024 should be rescinded and a new Bill be presented which was more harmonious to the rights of freedom of expression for Barbadians, citizens and residents alike.

Finally, Mr. Chairman disagreed with Mr. Weekes' previous claim that the Bill was being enacted to protect the rights of politicians and their friends. He stated that the CB, 2024 was to protect all persons from abuse and humiliation *via* social media platforms.

(v) Mr. Timon Howard, Student, University of the West Indies and Spoken Word Artist

Mr. Howard presented to the Committee that his main issue was in relation to the CB, 2024. Freedom of expression which he believed was a natural human right and was being violated under Cyber bullying, Clause 20.(1)(b). He stated that the defences as provided pursuant to Clause 19.(5) were clear but queried why this was not extended to the offences under Clause 20.(1)(b).

He was asked by Senator G. P. B. Nicholls his views as to whether the CB, 2024 puts any undue restrictions on artistic licence, and if so, how can vulnerable persons be protected by cybercrime? He submitted that he was concerned with some of the restrictions placed on the artistic licence particularly with commentary on social media. He suggested that provisions should be included in the Bill to protect artists who articulate and express themselves so as to avoid any criminal sanctions.

SUSPENSION

The meeting was suspended at 1:40 p.m. until 2:15 p.m. for the lunch break.

RESUMPTION

The Chairman resumed the meeting at 2:25 p.m.

(vi) Hon. Ms. Marsha K-A. Caddle, Minister of Industry, Innovation, Science and Technology

Hon. Ms. Marsha K-A. Caddle made the final oral presentation where she addressed a few of the concerns and presented some suggestions to the Committee. First, the issue of ethical hacking and to prevent unauthorised access to data or systems. She gave the assurance that Government would put regulations in place to rectify this issue.
Secondly, "Critical information infrastructure system", Clause 12.(1). She reported that it was mentioned that there was an exclusion of infrastructure systems relative to hospitality and should be included. Though it was not an exhaustive list, she stated that it could be amended by a Ministerial Order.

Thirdly, Hon. Minister Caddle proposed the following amendment in relation to "Malicious communications", Clause 19.(3): delete the words *'not caring whether they are true or false'* and substitute the words *'that are false'*; also delete the words, *'ridicule'* and *'contempt'*. Clause 19.(3) should now read: *'A person who intentionally uses a*

computer system to disseminate any image or words that are false, and causes or is likely to cause or subject a person to humiliation, embarrassment or reputational injury is guilty of an offence...'

Finally, she further proposed the following amendment in relation to "Cyber bullying", Clause 20.(1)(b): delete the words *'annoyance'*, *'inconvenience'*, *'obstruction'*, and *'insult'*. Clause 20.(1)(b) should now read: *'for the purpose of causing danger, embarrassment, injury, humiliation, intimidation, hatred, anxiety, or causes substantial emotional distress to that person,'...*

Members of the Committee questioned Hon. Minister Caddle on her oral submissions. Notably, she reiterated that the Bill is far reaching as it aims to protect people, their reputations, information and system; and by so doing the alleged perpetrator will meet criminal prosecution because of the intention to cause harm, injury and damage.

Hon. Minister Caddle was asked whether the Bill would capture persons within Canada, USA and England who would have committed alleged offences under the Bill and be charged. She answered in the affirmative and clarified that both Bills once passed allows the pursuit of gathering evidence and the preservation of data in jurisdictions outside of Barbados, as applicable.

Item 5: Any other Business

Mr. Chairman raised the issue of the expiration of the three (3) months' timeline to complete the report as the Committee's mandate expires on Thursday, May 16th, 2024. It was agreed that Senator Gregory P. B. Nicholls would request from the Senate an extension of time for the Committee to complete the report no later than June 7th, 2024 at the Honourable Senate's 45th Sitting on Wednesday, May 15th, 2024.

ADJOURNMENT

There being no other business, on the motion of Senator Gregory P. B. Nicholls seconded by Dr. Romel O. Springer, the meeting was adjourned until Thursday, May 23rd, 2024 at 10:00 a.m.

Mr. Chairman adjourned the meeting accordingly at 5:45 p.m.

Deputy Clerk of Parliament

Confirmed this 4th **day of** July **2024.**

Chairman

PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2022 - 2027)

JOINT SELECT COMMITTEE (STANDING)
ON GOVERNANCE AND POLICY MATTERS

Minutes of the Fifth meeting of the Joint Select Committee (Standing) on Governance and Policy Matters on the review and examination of the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024, held in the Senate Chamber, Parliament Buildings, Trafalgar Street, Bridgetown, St. Michael on Thursday, May 23rd, 2024 at 10:00 a.m.

PRESENT WERE:

Mr. Edmund G. Hinkson, S.C., M.P. **(Chairman)**
Mr. Peter R. Phillips, J.P., M.P.
Mr. Ralph A. Thorne, K.C., M.P.
Senator Gregory P. B. Nicholls
Senator the Hon. Lindell E. Nurse

IN ATTENDANCE WERE:

Mr Pedro Eastmond, *Clerk of Parliament*
Ms. Beverley S. Gibbons, *Deputy Clerk of Parliament*
Miss Suzanne Hamblin, *(Journal Department of Parliament)*

ABSENT:

Dr. Romel O. Springer, J.P., M.P.
Senator Ryan O. Walters
Mr Nigel Jones, *Deputy Clerk of Parliament*
Ms Rhea Drakes, *Parliamentary Counsel, Office of the Chief Parliamentary Counsel (Excused)*

Item 1: Call to Order and Welcome

The Meeting was called to order by the Chairman at 10:35 a.m. who welcomed all present.

Item 2: Minutes of the Fourth Meeting held on Monday, 13th May, 2024

On the motion of Senator G. P. B. Nicholls seconded by Mr P. R. Phillips the minutes were deferred.

Item 3: Matter Arising

There being no minutes the item was deferred.

Item 4: Consideration of Written Presentations

The Chairman informed the members that the discussion before the Committee was how best to manage the approximately 50 odd submissions that were received. He informed that while some of them were very short and some highlighting the same issues there are some key ones he had selected to proceed with discussion.

The Committee considered the following submissions

- **Barbados Bar Association (BAR).**

It was agreed that some of the suggestions of BAR have merit. Senator Nicholls however stated that the view of the BAR on the unconstitutionality of the Cybercrime Bill is a misreading of the law in *Hinds v R.* There was agreement that there was no need to hear orally from the BAR or The Barbados Bankers Association because of the degree of clarity of their submissions.

The Committee discussed the suggestion by the BAR that some of the fines should be lowered. It was agreed that the Court will make a determination as to whether to give the maximum penalty or any penalty in that range and therefore to lower the maximum narrows the scope of culpability. Senator Nurse queried how the determination of the fines are established. The Committee also discussed the suggestion that the Bill should have Regulations to govern enforcement.

- **Barbados Association of Journalist and Media Workers (BARJAM).**

The Chairman noted that the submission by BARJAM commented on the rate of fines in some cases. He stated that since the Minister made concessions to Clauses 19 and 20 that there is no need to

address them at this stage. The Chairman acknowledged the request from BARJAM for the 'Freedom of Information' legislation for the press but stated that it was not in the remit of this Committee. However, it can be discussed further in deliberations.

- **The Barbados Police Service (TBPS).**

The Committee noted that they did not raise any issues but just provided commentary on Clauses 19 and 20 of the Bill.

- **The Barbados Bankers Association (TBBA).**

The Chairman noted that the TBBA focused on where actions were taken without authority and recommended a definition of "without authority". He proposed to seek the guidance of the Office of Chief Parliamentary Counsel who was currently absent. He also noted that the TBBA also raised concerns that some of the Clauses were found to be too broad.

- **Barbados Consumer Empowerment Network (BCEN)**

The Chairman noted that it was the opinion of this submission that there was not enough consumer protection. He believed that this observation did not have merit as regards this particular Bill as opposed to other possible legislation.

- **Mr. Niel Harper**

The Committee deferred going through his presentation until the officer from the Chief Parliamentary Counsel was present.

- **Mr. Steven Williams**

The Chairman noted that Mr. Williams was generally in favour of the Bill as drafted. The Committee further noted the suggestion by Mr. Williams that critical infrastructure service provisions currently in Clause 12 be placed in Regulations for easier amendment. The Chair proposed that the list of 'critical infrastructure services' be expanded and that the committee would consider that extended list at a later meeting.

The Committee then considered the more general submissions.

The Chairman noted that most of the submissions spoke towards Clauses 19 and 20 being vague and seeking to curb the constitutional right to freedom of expression and that the Committee should concentrate its deliberations there. Senator Nicholls indicated to the Committee that the right to freedom of expression is not absolute and the Constitution provides for laws to be passed to reasonably limit that expression if it is required in the public interest. The Chairman sought to have clarity on the freedom of speech in Barbados versus the freedom of speech in the United States (US). The conclusion drawn by the Committee is that it is not within the same context.

The Chairman also raised the issue on whether the Committee wanted to consider proposing a defence in Clause 20. Senator Nicholls informed the Committee that he had looked at several pieces of legislation around the world and he did not find a definition for 'cyber bullying' in the various jurisdictions. He however noted that the Canada Criminal Code gives an explanation as to what is cyberbullying though it is not defined. Mr. R. Thorne opined that Clause 20 criminalizes simple language and needs to be worked on.

The Committee further discussed Clause 20. (1) as drafted with the discussion centred around whether 20.(1) *(a)* and 20.(1) *(b)* are intended to create separate offences. It was agreed that it will be left for explanation by the officer from the Chief Parliamentary Counsel.

The Committee then discussed the submission of Michelle Bayley in which she suggested amendment to some of the clauses of the Bill. The Chairman indicated that her suggestions are outside of the scope of what normally appears in legislation and thus the Committee determined that the submission was without merit.

The Committee agreed that in the interest of time to take the submissions as read and that the report will consist of a brief summary of all the submissions to be prepared by the Clerk and those submissions will be appended.

The Committee agreed to consider specific amendments to the Bill but noted that they would have to have the draftsperson present before finalizing.

- **Clause 13. (2).**

The Committee recommended that at paragraph '(b)', the word '*and*' be deleted and substituted with the word '**or**' to enable either of the defences without having to rely on all three.

- **Clause 23. (1).**

The Committee agreed with the recommendation that the words **'Judge or'** should be included before the word *'magistrate'* at line 5.

- **Clause 23. (2) *(d).***

The Committee noted that the Barbados Bankers Association Inc. (TBBA) had a concern with **Clause 23. (2)** paragraph ***(d)*** where they believed that "providing such code would endanger the security of other data which is not relevant to the offence, an option for the data to be decrypted for the officer should be an option" and that they recommended to the Committee that this clause should include protection for "privileged information or material" as is done under the *Proceeds and Instrumentalities of Crime* Act, 2019. It was suggested that that may be a policy decision and that it be referred to the Minister for comment.

- **Clause 19. (4).**

The Chairman noted the word 'intimidate" and that there is no defence and drew the Committee's attention to 19. (4) *(a)* (iii) which states "a person substantial emotional distress." He posed the question to the Committee as to whether that section should be deleted. The Committee agreed that it should remain.

The Chairman then summarised the areas that the Committee agreed to in principle:

- Clause 12, list of 'Critical information infrastructure systems' and recommended that the Committee add to the list.
- Clause 13, that the word "*and*" between (b) and (c) should be "**or**".
- In the interest of the BAR's comments and submissions, that the Committee consider making the offences under Clauses 19 and 20 not only by summary trial, but by indictment as well to avoid what the BAR considers a real possibility of constitutional challenge.
- Niel Harper's submission to be discussed in the presence of the draftsperson.

Item 5: Any Other Business

The Committee agreed that the next meeting would be held on Monday 27th May, 2024 and the draughtsperson from CPC, Ms Rhea Drakes would be available.

ADJOURNMENT

There being no further business, on the motion of Mr P. R. Phillips seconded by Senator the Hon. L E. Nurse the meeting was adjourned to Monday, May 27th, 2024 at 2:00 p.m.

The Chairman adjourned the meeting accordingly at 1:05 p.m.

Clerk of Parliament

Confirmed this 4th day of July 2024.

Chairman

(As amended)

PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2022 - 2027)

JOINT SELECT COMMITTEE (STANDING)
ON GOVERNANCE AND POLICY MATTERS

Minutes of the Sixth meeting of the Joint Select Committee (Standing) on Governance and Policy Matters on the review and examination of the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024, held in the Senate Chamber, Parliament Buildings, Trafalgar Street, Bridgetown, St. Michael on Monday, May 27th, 2024 at 2:00 p.m.

PRESENT WERE:

Mr. Edmund G. Hinkson, S.C., M.P. **(Chairman)**
Mr. Peter R. Phillips, J.P., M.P.
Dr. Romel O. Springer, J.P., M.P.
Mr. Ralph A. Thorne, K.C., M.P.
Senator Gregory P. B. Nicholls ***(Online)***
Senator the Hon. Lindell E. Nurse
Senator Ryan O. Walters

IN ATTENDANCE WERE:

Mr Pedro Eastmond, *Clerk of Parliament*
Ms. Beverley S. Gibbons, *Deputy Clerk of Parliament*
Miss Suzanne Hamblin, *(Journal Department of Parliament)*
Ms Rhea Drakes, *Parliamentary Counsel, Office of the Chief Parliamentary Counsel*

Item 1: Call to Order and Welcome

The Meeting was called to order by the Chairman at 2:18 p.m. who welcomed all present.

Item 2: Consideration of Oral Presentations

The Committee considered the oral submissions.

- **Mr. Niel Harper**

The Chairman drew the Committee's attention to Mr Harper's submission in which he indicated that Clause 5 'Modification of Programme or data" uses outdated language, that the clause is unnecessary and that the focus should be on someone who intentionally and without authority causes harm. Senator Nicholls queried what is the legislative intent.

Ms Drakes informed the Committee that Clause 5 is the existing law. She further clarified that section 3 subsections (3), (4) and (5) of the *Computer Misuse* Act Cap. 124 is incorporated into this Clause, redrafted using in a different format. She also noted that the draft Bill was created in connection with the Council of Europe and that it does not run afoul of the Budapest Convention. She stated that the Budapest Convention does not identify harm or the effect, as a consequence of the offence but that the person intentionally and without authority committed the offence.

The Committee also noted the opinion of Mr Harper which stated that Clauses 5 to 7 seeks to criminalise modern uses of software and data processing. This was also refuted by Ms Drakes as she stated it applies only if a person does not have the requisite permission or authority.

The Chairman raised the query highlighted in some of the submissions of the omission of the word 'recklessly' from some clauses but included in some. Ms Drakes noted that this was mostly a policy decision.

In relation to Mr Harper's comments on Clause 8, Ms Drakes informed the Committee that the text of the clause is aligned with the Budapest Convention. The Committee determined that his argument was not enough to lower the bar on the intent of the Bill.

The Committee in its discussion of Mr Harper's comment on Clause 9 considered a suggestion from Senator Nicholls to broaden the scope to include the words "knowledge, permission and consent". The Committee agreed to amend the Bill to include a definition of the term "without authority" in Clause 2 (5).

In relation to Clause 11, the Committee considered the argument by Mr Harper that this is not treated to in the other conventions. Ms Drakes informed that that Clause is currently in the *Computer Misuse* Act, 2005 and that the disclosure must be done intentionally or recklessly and without authority.

- **Mr Steven Williams**

The Committee considered two of the issues raised by Mr Williams. (1) That the Bill needs Regulations to which Ms Drakes responded and informed the Committee that Clause 30 of the Cybercrime Bill "provides that the Minister may make Regulations generally for the purpose of given effect to this Act." She noted that it is for the piloting Ministry to provide the policy to CPC who will then draft the Regulations; and

(2) The issue of sharing passwords with a third party could lead to a penalty under the Act. The Committee determined that they did not share the view.

- **Mr Anthony Green, General Manager, STARCOM Network**

The Committee agreed that most of Mr Green's presentation was geared toward freedom of information legislation and that he also spoke in relation to Clause 5 which prohibits illegal interception of data. They further noted his opinion that there should be an exception for journalist and media professionals if the publication is in the public interest. Ms Drakes explained that there is no criminal offence or penalty for receiving or publishing. The Committee agreed that Ms Drakes should draft a 'public interest' defence, not just for journalists but for any person acting in the public interest, for the consideration of the Committee.

- **Ms Janine Butcher**

The Chairman highlighted that her concern was the need to protect whistleblowers who may want to disclose information in the interest of the public and it was agreed that the Committee had already determined the defence of "public interest".

- **Mr. Timon Howard**

The Chairman noted that Mr Howard spoke to the fact that licence should be given for artistic commentary and that it should not attract criminal sanction. The Chairman again queried whether the 'public interest' defence did not apply here. Senator Nicholls suggested that that protection of the artistic commentary should be done at the policy level with the use of prosecutorial guidelines.

The Committee concluded that it had highlighted the most pertinent points from the submissions. The Chairman indicated to the Clerk that the legislation from Guyana, Jamaica and Belize which Ms Drakes had indicated all have similar provisions, framework and offences, be attached to the Report as guides.

The Committee determined that prosecutorial guidelines should also be attached to the report. Ms Drakes informed that Committee that the appropriate authority for the guidelines may be the office of the Director of Public Prosecutions (DPP).

Item 3: Consideration of the Bills.

The Chairman suggested that some of the clauses, certainly in Part II of the draft Cybercrime Bill are repeated in principle from the Computer Misuse Act and asked Ms. Drakes if she is aware of any prosecutions. She replied she was not but that information may be best gained from the office of the DPP.

The Chairman highlighted the query from The Barbados Bankers Association (TBBA) who posited that the Cybercrime Bill should include protection for privileged information or material as they claim is done under *Proceeds and Instrumentalities of Crime* Act and he asked Ms Drakes for a response. He noted that their concern was 23(2)(d), where, *"A warrant issued under this section may authorise a police officer to have access to any information, code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer system into readable comprehensible format or text, for the purpose of investigating any offence."* Ms Drakes informed the Committee that that would be a policy decision. She noted that there can be references or portions of legislation that are replicated in other legislation but she would have to seek further instructions from the parent Ministry.

The Clerk opined that the Committee could make a recommendation as relates to policy decisions noting that when the report is completed, the report goes back to the House of which it originated and that House then debates and adopts or rejects any suggestions or amendments proposed by the Committee. He noted that though Ms Drakes as drafter cannot act on things that hinge or touch and concern policy, the recommendation can be included in the report.

The Chair referenced Senator Nicholls' issue of a definition of cyberbullying in Clause 20 and noted his citation of the Canadian Legislation Criminal Code 1985.

The query as to whether Clause 20 (1) *(a)* and (*b*) are two separate offences or that *(b)* is a qualification on the conduct of *(a)* was raised with Ms Drakes. Her response was that it was more or less a qualification indicating that there are not two separate offences. She gave further clarity and recommended to the Committee that the '*(a)* and *(b)*' can be removed and have one sentence.

The Committee then considered Clause 13.(2) and suggested that the word "and" after the semicolon in (b) should be replaced with the word "or".

Item 4: Consideration of proposed amendments.

Clause 1 No change

Clause 2. (1) The word "Cyber bullying" was recommended by the Committee to be defined.

The Committee agreed with CPC's recommendation that for the purpose of clarity, '*without authority*' could be defined to state "it includes or it means without the person's permission and consent and to include in excess of the person's authority".

Clause 3. No change

Clause 4. "*Illegal access*"; **Clause 5.** "*Modification of programme or data*"; **Clause 6.** "*Interfering with programme or data*"; **Clause 7.** "*Interfering with computer system*"; **Clause 8.** "*Illegal interception of data*; **Clause 9.** "*Misuse of devices*"; and **Clause 11.** "*Disclosure of access code*" the

The Committee recommended that CPC draft an exception relative to *'public interest'* as a defence and stressed that it should not target any particular group noting that the Law Courts would determine the question of public interest.

Clause 10. No change

Clause 12. Critical information infrastructure system. The Committee discussed and agreed that it was not necessary to expand this list as this section was intentionally drafted in broad language to capture the agencies and sectors.

Clause 13. The Committee agreed to replace the "and" with "or".

Clauses 14 to 18 No Change

Clause 19. The Committee determined that the amendments to this section were already made when Minister Marsha Caddle appeared before the Committee.

Clause 20. (1) The Committee earlier agreed to remove the *(a)* and *(b)* and have one paragraph.

Clause 21 to 22. No Change

Clause 23. (1) The Committee agreed with the recommendation that the words ***'Judge or'*** should be included before the word *'magistrate'* at line 5.

The Committee reverted and discussed extensively the fines in Clauses 19 and 20 and concluded to have them as indictable but leave the fines as is.

Clause 23(2)(a). The Committee recommended that the words, ***"or contains evidence"*** be inserted before the words *'that an offence has been or is about to be committed;'*

Clauses 24 to 33 The Committee deemed them to be without requirement for amendment.

The Committee considered the ***Mutual Assistance in Criminal Matters (Amendment)*** Bill, 2024 and no amendments were suggested.

Item 5: Any Other Business

It was agreed that the proposed amendments to the Bill as suggested by the Committee would be formulated by the Clerk and submitted to the parent ministry for consultation on policy decisions. The Committee would then meet to agree on the proposed changes to the legislation and sign off on the report.

ADJOURNMENT

There being no further business, on the motion of Mr P. R. Phillips seconded by Senator the Hon. L E. Nurse the meeting adjourned s*ine die*.

The Chairman adjourned the meeting accordingly at 5:30 p.m.

Pedro. L. Eastmond
Clerk of Parliament

Confirmed this 4th day of July 2024.

Richmond B. Nixon
Chairman

PARLIAMENT OF BARBADOS
(FIRST SESSION OF 2022 - 2027)

JOINT SELECT COMMITTEE (STANDING)
ON GOVERNANCE AND POLICY MATTERS

Minutes of the Seventh meeting of the Joint Select Committee (Standing) on Governance and Policy Matters on the review and examination of the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024, held in the Senate Chamber, Parliament Buildings, Trafalgar Street, Bridgetown, St. Michael on Thursday, July 4th, 2024.

PRESENT WERE:

Mr. Edmund G. Hinkson, S.C., M.P. **(Chairman)**
Mr. Peter R. Phillips, J.P., M.P.
Dr. Romel O. Springer, J.P., M.P.
Mr. Ralph A. Thorne, K.C., M.P.
Senator the Hon. Lindell E. Nurse
Senator Ryan O. Walters

IN ATTENDANCE WERE:

Mr Pedro Eastmond, *Clerk of Parliament*
Ms. Beverley S. Gibbons, *Deputy Clerk of Parliament*
Miss Suzanne Hamblin, *(Journal Department of Parliament)*

ABSENT

Senator Gregory P. B. Nicholls (*Excused*)
Ms Rhea Drakes, *Parliamentary Counsel, Office of the Chief Parliamentary Counsel (Excused)*

Item 1: Call to Order and Welcome

The Meeting was called to order by the Chairman at 2:45 p.m. who welcomed all present.

Item 2: Minutes of the following meetings:

The minutes of the following meetings were considered, corrected and amended in particular as follows;

- **Third meeting – Monday 6th May, 2024**

Page 2, in the first paragraph under the heading *'(i) Mr Neil Harper'* delete the first lowercase 'c" in the word '*cybercrime*' and replace same with a capital "**C**".

Page 3, line 11, insert a full stop after the word '*Convention*' and delete the word 'and' after the word *'Convention'*.

Page 3, line 12, delete the word '*and*' and substitute the word "**is**" therefor.

Page 4, line 4, the word "**to**" was inserted between the words '*relation*' and '*this*'.

Page 5, line 6, delete the word '*action*' and substitute the words "**actions which**" therefor.

Page 6, paragraph 3, line 5, insert the words "**as it currently exists**" after the word '*media*' and before the words '*and the intention*'.

Page 7, paragraph 3, the name '*Caswel Franklyn*' was corrected to read "**Caswell Franklyn**"

Page 7, paragraph 4, line 2, insert the word "**Bill**" between the words '*the*' and '*to address*', in line 3, substitute the word "**have**" for the word '*had*' and, in line 5, substitute the word "**designated**" for the word '*designating*'.

On the motion of Dr. R. O. Springer seconded by Mr. P. R. Phillips the minutes were confirmed as amended.

- **Fourth Meeting – Monday 13th May, 2024**

Page 3, paragraph 2, the sentence '*Finally, she stressed that she wanted to see the establishment of independent oversight bodies separate and distinct from the law enforcement agencies.*' was deleted. In line 3 insert the word "**final**" between the word '*this*' and the word '*recommendation*'.

Page 5, first paragraph, line 2, delete the word 'and'.

Page 6, paragraph 4, line 1, delete the word '*Finally*' at the beginning of the sentence. In paragraph 5 the word "**alleged**" was inserted between the words '*committed*' and '*offences*'.

Page 7 paragraph 1, insert the words "**from the Senate**" between the words '*extension*' and '*of time*'.

On the motion of Dr. R. O. Springer seconded by Mr. P. R. Phillips the minutes were confirmed as amended.

- **Fifth Meeting – Thursday 23rd May, 2024**

Page 3, paragraph 4, the second sentence was deleted and the following was substituted therefor "**He believed that this observation did not have merit as regards this particular Bill as opposed to other possible legislation**."

Page 5, under the third bullet point '*Clause 19(4)*' in paragraph 2, line 5 the word '*Association's*' was deleted and the word BAR was amended to read "**BAR's**", and in line 9, the words "**to be discussed**" were inserted between the words '*submission*' and '*in*'.

On the motion of Mr. P. R. Phillips seconded by Dr. R. O. Springer the minutes were confirmed as amended.

- **Sixth Meeting – 27th May, 2024**

Page 4, paragraph 4, line 9 the word '*potions*' was corrected to **"portions"**.

On the motion of Mr. P. R. Phillips seconded by Dr. R. O. Springer the minutes were confirmed as amended.

Item 3: Matters arising

Matters Arising were previously considered during the confirmation of the respective minutes.

Item 4: Consideration of the amendment to the Bill

The Chairman indicated that he had requested comments from the office of the Director of Public Prosecutions (DPP) and queried as to whether the members of the Committee had seen the response. He suggested that that response be included in the report. The Committee agreed.

The Committee considered the amendments to the Cybercrime Bill, 2024 dated 2024-06-18 as amended by the office of the Chief Parliamentary Counsel (CPC) and which was circulated to members.

Amendments

Clause 2. (1)

"cyber bullying" means the behaviour or conduct referred to at section 20;

The Committee agreed to this amendment.

"without authority" means without right, consent, permission, authorization or in excess of authorization.

The Committee discussed at length the concept of authorisation, the level of and from whom it can be rightfully issued. The definition in the Bill as proposed by the CPC was accepted.

Clause 4. to 11. (with the exception of Clauses 9. and 10.)

The provision that:
"It shall be a defence to a charge brought under subsection (1) if the person establishes that the access to a computer system, programme or data was in the public interest."

The Committee took the decision that the exception relative to *'public interest'* as a defence be deleted.

Clause 13. (2) (b)

"was subject to legal privilege; **or** ..."

The Committee agreed to the amendment.

Clauses 19. and **20.**

The Committee agreed that as per the amendment to the *Criminal Procedure* Act the recommendation is that this legislation provide hybrid offences and the accused has the option to choose to be tried by a Judge or a Magistrate. The Chairman suggested that the language be drafted similar to

that used by the legislation of Guyana, Belize or British Virgin Islands and similarly proposed that this amendment also apply to Clause 20.

The Chairman also recommended that the penalties be hybrid and that the penalties match the mode of trial.

The Committee therefore agreed that for Clauses 19. and 20. should be amended to read

"A person who ... **is guilty of an offence the penalty should be on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both."**

The Chairman proposed that the word 'embarrassment' which was previously deleted from Clause 19. but not from Clause 20. be reinserted into Clause 19. After much discussion the Committee voted by majority for the removal of the word "embarrassment" from Clause 20 as well.

Clause 23. (1)

The Committee agreed to the inclusion of the words **"Judge or"**.

Clause 23(2)(a)

The Committee approved the insertion of the words, **"or contains evidence".**

Clause 23.(6)

The Committee discussed the amendment inserted in this clause which emanated out of the submission by The Barbados Bankers Association (TBBA), to have privileged information as applies under the *Proceeds of Instrumentalities and Crime* Act. The Chair indicated that this amendment as drafted does not add to the existing convention as it relates mainly to attorney client privilege and proposed that it should be deleted. The Committee agreed that Clause 23. (6), (7) and (8) be deleted and to the consequential renumbering of the sub-sections following.

Item 5: Consideration of the Report

In response to the request from the Chairman the Clerk of Parliament, Mr Pedro Eastmond indicated that work had started on the report and gave a brief synopsis of what it would entail including all submissions sent to the Committee. The Chairman suggested that the report should also include the Prosecutorial Guidelines from Jamaica. It was noted that the amendments made would have to be sent to CPC to have the Bill further amended and be resubmitted to the Committee.

Item 6: Any Other Business

The Committee was informed that an extension was granted to August 7th for the Committee to report but that the Office of the Clerk of Parliament would endeavour to complete the report by the end of July.

ADJOURNMENT

There being no further business, on the motion of Mr P. R. Phillips seconded by Dr. R. O. Springer the meeting was adjourned *sine die*.

The Chairman adjourned the meeting accordingly at 4:31 p.m.

for **Clerk of Parliament**

Confirmed this 25th day of July 2024.

Chairman

CYBERCRIME BILL, 2024

2024-01-29

OBJECTS AND REASONS

This Bill would provide for

(a) the combatting of cybercrime;

(b) the protection of legitimate interests in the use and development of information technologies;

(c) the facilitation of international co-operation in computer related crimes;

(d) the repeal of the *Computer Misuse Act*, Cap. 124B; and

(e) related matters.

Arrangement of Sections

PART I

PRELIMINARY

PART II

PROHIBITED CONDUCT

BARBADOS

A Bill entitled

An Act to provide for the combatting of cybercrime, protection of legitimate interests in the use and development of information technologies, the facilitation of international co-operation in computer related crimes and related matters.

ENACTED by the Parliament of Barbados as follows:

PART I

PRELIMINARY

Short title

1. This Act may be cited as the *Cybercrime Act, 2024.*

Interpretation

2.(1) In this Act,

"approved person" means a person who has the relevant training and skill in computer systems and technology, who has knowledge about the functioning of the computer system and is identified, in writing, by the Commissioner of Police or other gazetted officer designated by the Commissioner, to assist the police;

"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function;

"computer data storage medium" means any article or material from which electronic information is capable of being reproduced, with or without the aid of any other electronic article or device;

"computer programme" or "programme" means data or a portion of data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer system" means a device or a group of inter-connected or related devices, one or more of which, pursuant to a programme, facilitates communication, performs automatic processing of data or any other function;

"damage" includes

(a) any impairment to the integrity of a computer system or the integrity or availability of any data or programme held in a computer system; and

(b) the impairment of the confidentiality of data or programme held in a computer system;

"intercept" includes, in relation to a computer system, listening to, monitoring or surveillance of or recording a function of a computer system, or acquiring the substance, meaning or purport of the function;

"service provider" means

(a) a public or private entity that provides to users of its services the ability to communicate by means of a computer system; and

(b) any other entity that processes or stores computer data on behalf of that entity or its users;

"ship" means a vessel which is designed, used or capable of being used solely or partly for navigation in, on, through, or immediately above the water, without regard to method or lack of propulsion and includes a maritime autonomous surface ship;

"traffic data" means computer data that

(a) relates to a communication by means of a computer system;

(b) is generated by a computer system that is part of a chain of communication; and

(c) shows the origin, destination, route, time, date, size, duration of the communication or the type of underlying services.

(2) For the purposes of this Act, access of any kind by a person to any computer system, programme or data is obtained without authority if he knows that he is

not entitled to access of the kind in question relating to the computer system, programme or data and

(a) he accesses the computer system, programme or data; or

(b) he exceeds any right or permission to access the computer system, programme or data from any person who may permit such access.

(3) A reference in this Act to any "programme or data" held in a computer system includes a reference to

(a) any programme or data held in any removable storage medium which is for the time being in the computer system; or

(b) any programme or data held in any storage medium which is external to the computer system, but which is connected to it.

(4) For the purposes of this Act, a modification of the contents of any computer system takes place if, by the operation of any function of the computer system concerned or of any other computer system

(a) any programme or data held in the computer system is altered or erased;

(b) any programme or data is added to any programme or data held in the computer system; or

(c) any act occurs which impairs the normal operation of any computer system,

and any act which contributes towards such a modification shall be regarded as causing it.

(5) Any modification referred to in subsection (4) is without authority if the person whose act causes the modification

(a) knows that he is not entitled to determine whether the modification should be made; and

(b) has not obtained the consent of the person who is entitled to consent to the modification.

(6) A reference in this Act to a programme includes a reference to a part of a programme.

Application

3.(1) This Act applies to an act done or an omission made

(a) in Barbados;

(b) on a ship or aircraft registered in Barbados; or

(c) by a national of Barbados outside the territory of Barbados, if the person's conduct would also constitute an offence under the law of a country where the offence was committed.

(2) For the purpose of paragraph *(a)* of subsection (1), an act is carried out in Barbados if

(a) the person is in Barbados when the act is committed; or

(b) the person is outside Barbados at the time when the act is committed but

(i) a computer system located in Barbados or electronic data storage medium located in Barbados is affected by, or contains information about the act; or

(ii) transmission or effect of the act, or the damage resulting from the act, occurs in whole or in part within Barbados.

(3) The *Mutual Assistance in Criminal Matters Act*, Cap. 140A shall apply to this Act in relation to an offence under this Act as if the offence were a serious offence within the meaning of section 2 of that Act.

PART II

PROHIBITED CONDUCT

Illegal access

4.(1) A person who intentionally or recklessly and without authority,

(a) gains access to the whole or any part of a computer system;

(b) causes a programme to be executed; or

(c) uses a programme to gain access to any data,

is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

(2) For the purposes of subsection (1), the form in which any programme or data is accessed or obtained and, in particular, whether or not it represents a form in which it is capable of being executed is immaterial.

Modification of programme or data

5.(1) A person who intentionally or recklessly and without authority causes any modification to a programme or data is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) For the purposes of subsection (1), the act in question need not be directed at

(a) any specifically identifiable programme or data or type of programme or data; or

(b) any programme or data that is held in a specifically identifiable computer system.

(3) For the purposes of subsection (1), it is immaterial whether the modification is or is intended to be permanent or temporary.

Interfering with programme or data

6.(1) A person who intentionally or recklessly and without authority,

(a) copies or moves a programme or data

(i) to any storage medium other than that in which that programme or data is held; or

(ii) to a different location in the storage medium in which that programme or data is held;

(b) destroys or erases a programme or data;

(c) damages a programme or data;

(d) suppress a programme or data;

(e) adds, deletes or alters a programme or data;

(f) renders a programme or data meaningless, useless or ineffective;

(g) obstructs, interrupts or interferes with the lawful use of a programme or data; or

(h) denies access to a programme or data,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.

(3) For the purposes of subsection (1), the form in which a programme or data is copied and, in particular, whether or not it represents a form in which it is capable of being executed is immaterial.

Interfering with computer system

7. A person who intentionally or recklessly and without authority,

(a) hinders the functioning of a computer system by

(i) causing electromagnetic interference to a computer system;

(ii) accessing or causing access to a computer system; or

(iii) corrupting a computer system by any means; or

(b) interferes with the functioning of a computer system,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Illegal interception of data

8. A person who intentionally and without authority, undertakes an act to intercept by technical means any non-public transmission to, from or within a computer system, including electromagnetic emissions from a computer system carrying computer data, is guilty of an offence and is liable on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

Misuse of devices

9. A person who intentionally or recklessly and without authority,

(a) produces, sells, procures for use, imports, exports, distributes or otherwise makes available

(i) a device, including a computer programme, that is primarily designed or adapted for the purpose of committing an offence; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being

accessed, with the intent that it be used by any person for the purpose of committing an offence; or

(b) has an item mentioned in paragraph (*a*)(i) or (ii) in his possession with the intent that it be used by himself or any other person for the purpose of committing an offence,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Access with intent to commit further offence

10. A person who intentionally and without authority uses a computer system to perform any function in order to secure access to any programme or data held in that computer system or in any other computer system with the intention to commit a further offence is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Disclosure of access code

11.(1) A person who intentionally or recklessly and without authority discloses any password, access code or any other means of gaining access to any programme or data held in a computer system is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 3 years or to both.

(2) A person who intentionally or recklessly and without authority discloses any password, access code or any other means of gaining access to any programme or data held in a computer system for any unlawful gain, whether to himself or to another person, knowing that it is likely to cause unlawful damage, is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Critical information infrastructure system

12.(1) For the purposes of this section "critical information infrastructure system" means any computer system, programme or data that supports or performs a function that relates to

(a) electricity generation or distribution**;**

(b) telecommunications;

(c) government services;

(d) emergency services;

(e) law enforcement, security or intelligence agencies;

(f) public works; or

(g) any computer system, programme or data that may be designated as a critical information infrastructure system by the Minister responsible for the prevention of cybercrime, published in the *Official Gazette*,

that is so vital that the incapacity or destruction of such computer system, programme or data would have a debilitating impact on the security, national economic security, national public health or safety or any combination of those matters, in Barbados.

(2) A person who without authority,

(a) gains access to; or

(b) interferes with

a critical information infrastructure system is guilty of an offence and is liable on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

(3) A person who without authority gains access to or interferes with a critical information infrastructure system in the course of the commission of any offence

is liable on conviction on indictment to a fine of $150 000 or to imprisonment for a term of 12 years or to both.

(4) It shall be a defence to a charge brought under subsection (2) or (3) to prove that access to or interference with a critical information infrastructure system was obtained inadvertently and with no intent to commit an offence.

Receiving or giving of access to computer programme or data

13.(1) A person who

(a) intentionally or recklessly and without authority receives or is given access to any programme or data; and

(b) knows or believes that

(i) the programme or data was obtained without authority; or

(ii) access to the programme or data was obtained without authority,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) It shall be a defence to a charge brought under subsection (1) to prove that the programme or data or access to the programme or data

(a) was received inadvertently and with no intent to commit an offence;

(b) was subject to legal privilege; and

(c) was received by a law enforcement officer in the course of an investigation.

Computer-related forgery

14. A person who intentionally and without authority, inputs, alters, deletes or suppresses a programme or data that results in inauthentic data being considered or acted on for any legal purpose as if it were authentic, whether or not the data is directly readable and intelligible, is guilty of an offence and liable

on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

Computer-related fraud

15. A person who intentionally, fraudulently or dishonestly and without authority, inputs, alters, deletes or suppresses any computer data or interferes with the functioning of a computer system for the purpose of

(a) procuring an economic benefit for himself or another person;

(b) causing loss of property to a person;

is guilty of an offence and is liable on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

Child pornography

16.(1) A person who intentionally or recklessly

(a) publishes child pornography through a computer system;

(b) produces child pornography for the purpose of its publication through a computer system;

(c) possesses child pornography in a computer system or on a computer data storage medium for the purpose of publication; or

(d) procures child pornography through a computer system for himself or for another person,

is guilty of an offence and is liable on conviction on indictment

(i) in the case of an individual to a fine of $100 000 or to imprisonment for a term of 10 years or to both; or

(ii) in the case of a corporation, to a fine of $250 000.

(2) It shall be a defence to a charge brought under subsection (1) if the person establishes that the child pornography was for a *bona fide* research, medical or law enforcement purpose.

(3) For the purposes of subsection (1),

(a) “child” means a person under the age of 18 years;

(b) "child pornography" includes material that visually depicts

(i) a child engaged in sexually explicit conduct;

(ii) a person who appears to be a child engaged in sexually explicit conduct; or

(iii) realistic images representing a child engaged in sexually explicit conduct; and

(c) "publish" includes

(i) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(ii) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph *(b)*; or

(iii) print, photograph, copy or make in any other manner, whether of the same or of a different kind or nature, for the purpose of doing an act referred to in paragraph *(b)*.

Child grooming

17. A person who intentionally or recklessly uses a computer system to befriend, manipulate, communicate with or establish a connection with a child in order to abuse the child, whether sexually or otherwise, is guilty of an offence and is liable on conviction on indictment

(a) in the case of an individual to a fine of $100 000 or to imprisonment for a term of 10 years or to both; or

(b) in the case of a corporation, to a fine of $250 000.

Online child sexual abuse

18.(1) A person who intentionally or recklessly uses a computer system to meet a child for the purpose of

(a) engaging in sexual activity with a child;

(b) engaging in sexual activity with the child where

(i) coercion, inducement, force or threat is used;

(ii) a recognised position of trust, authority or influence over the child, including within the family is abused; or

(iii) a child's mental or physical disability or situation of dependence is abused

is guilty of an offence.

(2) A person who is guilty of an offence under subsection (1) is liable on conviction on indictment

(a) in the case of an individual to a fine of $100 000 or to imprisonment for a term of 10 years or to both; or

(b) in the case of a corporation to a fine of $250 000.

Malicious communications

19.(1) A person who intentionally or recklessly uses a computer system to publish, broadcast or transmit computer data that

(a) intimidates a person; or

(b) threatens to

(i) use violence towards a person or a member of his family; or

(ii) damage the property of a person or the property of his family,

is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) A person who intentionally or recklessly uses a computer system

(a) to publish, broadcast or transmit data that includes private sexual photographs and videos without the consent of a person who appears in them, with intent to humiliate, harass or cause substantial emotional distress to that person; or

(b) to send repeatedly to another person data that is obscene, vulgar, profane, lewd or indecent with intent to humiliate or harass the other person to the detriment of that person's health, emotional well-being, self-esteem or reputation,

is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(3) A person who intentionally uses a computer system to disseminate any image or words, not caring whether they are true or false, and causes or is likely to cause or subject a person to ridicule, contempt or embarrassment, is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(4) For the purposes of subsection (1),

(a) "intimidate" means to cause

(i) in the mind of a reasonable person injury to himself, any member of his family or any of his dependants;

(ii) in the mind of a reasonable person an apprehension of violence or damage to any person or property; or

(iii) a person substantial emotional distress;

(b) "injury" includes injury or damage to a person in respect of his business, occupation, profession, employment or other source of income.

(5) The defences of truth, comment, triviality and privilege, whether absolute or qualified, provided for under the *Defamation Act*, Cap. 199 shall extend to a prosecution under subsection (3).

Cyber bullying

20.(1) A person who intentionally uses a computer system

(a) to publish, broadcast or transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene or of a menacing character or causes any such data to be so sent;

(b) for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress to that person,

is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act

(a) for a *bona fide* scientific or medical research or law enforcement; or

(b) in compliance of and in accordance with the terms of a court order issued in exercise of any power under this Act or any law.

Cyber terrorism

21.(1) A person who intentionally uses or causes to be accessed a computer system for the purpose of terrorism is guilty of an offence and is liable on conviction on indictment to imprisonment for a term of 25 years.

(2) For the purposes of this section, “terrorism” has the meaning assigned to it in section 3 of the *Anti-Terrorism Act*, Cap. 158.

Aiding or abetting

22. A person who aids or abets the commission of an offence under this Act is guilty of that offence and is liable to the penalty of that offence.

PART III

INVESTIGATION AND ENFORCEMENT

Search and seizure

23.(1) Where a Judge or magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for suspecting that an offence has been, is being or is about to be committed in any place and that there is evidence that such an offence has been, is being or is about to be committed in that place, the magistrate may issue a warrant authorising any police officer to enter and search that place, including any computer system, using such reasonable force as is necessary.

(2) A warrant issued under this section may authorise a police officer to

(a) seize or similarly secure any computer system, data, programme, information, document or thing if he reasonably believes that it is evidence that an offence has been or is about to be committed;

(b) inspect and check the operation of any computer system referred to in paragraph *(a)*;

(c) use or cause to be used any computer system referred to in paragraph *(a)* to search any programme or data held in or available to such computer system;

(d) have access to any information, code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer system into readable and

comprehensible format or text, for the purpose of investigating any offence;

(e) convert an encrypted programme or data held in another computer system at the place specified in the warrant, where there are reasonable grounds for believing that computer data connected with the commission of the offence may be stored in that other system;

(f) make and retain a copy of any programme or data held in the computer system referred to in paragraph *(a)* or *(e)* and any other programme or data held in the computer system;

(g) maintain the integrity of the relevant stored computer data; and

(h) render inaccessible or remove computer data from the computer system.

(3) Where a Judge or magistrate is satisfied on the basis of an application by the Commissioner of Police or other gazetted officer that specified computer data or other information is required for the purpose of a criminal investigation or criminal proceedings, the Judge or magistrate may order a person who has knowledge about the functioning of a computer system or measures applied to protect the computer data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the measures in subsections (1) and (2).

(4) A warrant issued under this section shall authorise an approved person or a person who has knowledge about the functioning of a computer system or measures applied to protect the computer data to assist a police officer in the execution of the warrant.

(5) A person who obstructs a police officer in the execution of his duty under this section or who fails to comply with a request under this section is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 2 years or to both.

(6) For the purposes of this section,

"encrypted programme or data" means a programme or data which has been transformed from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such programme or data occurs or can be found, for the purpose of protecting the content of such programme or data;

"plain text version" means a programme or original data before it has been transformed to an unreadable or incomprehensible format.

Assisting a police officer

24.(1) A person who

(a) is in possession or control of a computer data storage medium or computer system; or

(b) has knowledge about the functioning of a computer system or measures applied to protect the computer data therein,

that is the subject of a search or a seizure, shall assist a police officer in the execution of a warrant issued under section 23.

(2) The assistance referred to in subsection (1) may include the following:

(a) accessing and using a computer system or computer data storage medium to search any computer data available to or in the system;

(b) obtaining and copying computer data referred to in paragraph *(a)*;

(c) using equipment to make copies;

(d) obtaining access to decryption information necessary to decrypt computer data required for the purpose of investigating the commission of the offence;

(e) obtaining an intelligible output from a computer system in a plain text format that can be read by a person;

(f) maintaining the integrity of the computer data; and

(g) rendering inaccessible or removing computer data in the computer system.

(3) A person who fails without lawful excuse or justification to assist a police officer in accordance with subsection (1) is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 2 years or to both.

(4) A person who seeks to prevent or prevents another person from assisting a police officer in the execution of a warrant issued under section 23 is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 2 years or to both.

(5) For the purposes of this section, "decryption information" means information or technology that enables a person to readily transform an encrypted programme or data from its unreadable and incomprehensible format to its plain text version.

Record of seized data to be provided to owner

25.(1) Where a computer system or computer data has been removed or rendered inaccessible to the owner or person who has control of the system following a search or a seizure under section 23, the person who made the search shall, at the time of the search or as soon as practicable after the search,

(a) make a list of what has been seized or rendered inaccessible, with the date and time of the seizure; and

(b) give a copy of that list to

(i) the owner of the computer system or computer data;

(ii) the occupier of the premises; or

(iii) the person in control of the computer system or computer data.

(2) Subject to subsection (3), a police officer or an approved person shall, on request,

(a) permit a person who had the custody or control of the computer system, or someone acting on behalf of that person, to gain access to and copy computer data on the system; or

(b) give the person referred to in paragraph *(a)*, a copy of the computer data.

(3) A police officer or an approved person may refuse to give access to or provide copies of computer data referred to in subsection (2) if he has reasonable grounds for believing that giving the access or providing the copies

(a) would constitute a criminal offence; or

(b) would prejudice

(i) the investigation in connection with which the search and seizure was carried out;

(ii) another investigation connected to the one in respect of which the search and seizure was carried out; or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

Production of data for criminal proceedings

26.(1) Where a Judge or magistrate is satisfied on the basis of an application by a police officer that specified computer data or other information is required for the purpose of a criminal investigation or criminal proceedings, the Judge or magistrate may order that

(a) a person shall submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; or

(b) a service provider offering services in Barbados produce subscriber information relating to such services that is in the service provider's possession or control.

(2) A person referred to in subsection (1) who discloses without authority any information in his possession or under his control is guilty of an offence and is liable on conviction on indictment,

(a) in the case of an individual, to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or

(b) in the case of a corporation, to a fine of $250 000.

(3) For the purposes of subsection (1), "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic or content data, which can establish

(a) the type of communication service used;

(b) the technical provisions taken relating to the communication service;

(c) the period of service;

(d) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information on the basis of the service agreement or arrangement; and

(e) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Expedited preservation and partial disclosure of traffic data

27. Where a Judge or magistrate is satisfied on the basis of an *ex parte* application by the Commissioner of Police or other gazetted officer that specified data stored in a computer system is required for the purpose of a criminal

investigation or criminal proceedings, the Judge or magistrate may make an order to ensure that expeditious

(a) preservation of traffic data is available regardless of whether one or more service providers was involved in the transmission of that communication; and

(b) disclosure of a sufficient amount of traffic data is given to enable the identification of

(i) the service providers; and

(ii) the path through which the communication was transmitted.

Preservation of data for criminal proceedings

28.(1) The Commissioner of Police or any other gazetted officer may make an *ex parte* application for a preservation order to a Judge or magistrate where

(a) computer data, including traffic data, stored in a computer system is required for the purposes of a criminal investigation; and

(b) there are grounds to believe that the computer data, including traffic data, stored in a computer system is particularly vulnerable to loss or modification.

(2) Where the Commissioner of Police or any other gazetted officer satisfies a Judge or magistrate on the basis of an *ex parte* application made under subsection (1), the Judge or magistrate may make an order requiring the person in control of the computer system to

(a) ensure that the computer data specified in the order is preserved for a period of up to 90 days;

(b) maintain the integrity of the computer data for a period of up to 90 days; and

(c) keep confidential any information or action relating to the preservation order.

(3) Where the Commissioner of Police or other gazetted officer makes an *ex parte* application for an extension of a preservation order, a Judge or magistrate may extend the preservation order beyond the 90 day period for a further period of up to 90 days.

Order for payment of compensation

29.(1) The Court may make an order for the payment of compensation where a person is convicted of any offence and he causes damage to another person's computer system, programme or data.

(2) A claim by a person for damages sustained by reason of the offence is deemed to have been satisfied to the extent of any amount which has been paid to that person under an order for compensation.

(3) An order made under subsection (1) shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(4) An order for compensation under this section is recoverable as a civil debt.

(5) For the purposes of this section, a programme or data held in a computer system is deemed to be the property of the owner of the computer system.

Regulations.

30. The Minister may make regulations generally for the purpose of giving effect to this Act.

Consequential amendments

31. The enactments set out in the first column of the *Schedule* are amended in the manner set out opposite thereto in the second column.

Repeal

32. The *Computer Misuse Act*, Cap. 124B is repealed.

Commencement

33. This Act shall come into operation on a date to be fixed by Proclamation.

SCHEDULE

(Section 31)

CONSEQUENTIAL AMENDMENTS

Column 1	Column 2
Enactment	*Amendment*
Copyright Act, Cap. 300	In section 31
	(a) delete subsection (5) and substitute the following: "(5) Copyright in a work is infringed by a person who, without the licence of the copyright owner, transmits the work by means of a computer system or telecommunications system (otherwise than by broadcasting or inclusion in a cable programme service) knowing or having reason to believe that infringing copies of the work will be made by means of the reception of the transmission in Barbados or elsewhere.".
	(b) insert immediately after subsection (5) the following new subsection: "(5A) For the purposes of subsection (5) "computer system" means a device or a group of interconnected or related devices, one or more of which, pursuant to a programme, facilititates communication, performs automatic processing of data or any other function.".

Schedule - (Concl'd)

CONSEQUENTIAL AMENDMENTS - *(Concl'd)*

Column 1 *Enactment*	Column 2 *Amendment*
Defamation Act, Cap. 199	Section 34 is deleted.
Extradition Act, Cap. 189	*(a)* In section 4, insert immediately after subsection (2) the following new subsection: "(3) An order made under subsection (2) shall be subject to affirmative resolution.". *(b)* In the *Schedule* insert immediately after paragraph 40 the following new paragraph: "41. Any offence under the *Cybercrime Act*, 2024 (2024-).".

Read three times and passed the House of Assembly this day of , 2024.

Speaker

Read three times and passed the Senate this day of , 2024.

President

MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024

2024-01-29

OBJECTS AND REASONS

This Bill would amend the *Mutual Assistance in Criminal Matters Act*, Cap. 140A to make provision for mutual assistance in matters relating to computer-related crimes and for related matters.

Arrangement of Sections

BARBADOS

A Bill entitled

An Act to amend the *Mutual Assistance in Criminal Matters Act*, Cap. 140A to make provision for mutual assistance in matters relating to computer-related crimes and for related matters.

ENACTED by the Parliament of Barbados as follows:

Short title

1. This Act may be cited as the *Mutual Assistance in Criminal Matters (Amendment) Act, 2024*.

Amendment of section 18 of Cap. 140A

2. ***Section 18 of the Mutual Assistance in Criminal Matters Act, Cap. 140A in this Act referred to as the principal Act is amended by***

(a) ***inserting immediately after subsection (3) the following new subsections:***

"(3A) Where an action on a request for assistance would prejudice a criminal investigation or a criminal proceeding conducted by its authorities, the central authority for Barbados may postpone an action.

(3B) Before refusing or postponing assistance, the central authority for Barbados shall, where appropriate after having consulted with the Commonwealth country, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

(3C) The central authority for Barbados shall

(a) promptly inform the Commonwealth country of the outcome of the execution of a request for assistance;

(b) give reasons for any refusal or postponement of the request; or

(c) inform the Commonwealth country of any reasons that render impossible the execution of the request or are likely to delay it significantly.";

(b) ***deleting subsection (4) and substituting the following:***

"(4) Where a Commonwealth country makes a request for assistance, the central authority for Barbados may supply information or material on the condition that it is

(a) kept confidential; or

(b) not used for investigations or proceedings other than those stated in the request for assistance."; and

(c) ***inserting immediately after subsection (4) the following new subsections:***

"(4A) Where a Commonwealth country cannot comply with a condition referred to in subsection (4), it shall promptly inform the central authority for Barbados.

(4B) Where a Commonwealth country has informed the central authority for Barbados that it is unable to comply with a condition under subsection (4), the central authority for Barbados shall determine whether the information is to be provided.

(4C) A Commonwealth country that accepts a condition in accordance with subsection (4) shall be bound by it.

(4D) Where the central authority for Barbados supplies information or material subject to a condition referred to in subsection (4), it may require the Commonwealth country to explain, in relation to that condition, the use made of such information or material.

(4E) Where, in the opinion of the central authority for Barbados, the expense involved in complying with a request for assistance would be of an extraordinary nature, the central authority for Barbados

(a) shall consult with the central authority for the country as to the terms and conditions under which compliance with the request may continue; or

(b) may refuse to continue further with the request in the absence of an agreement as to the terms and conditions for compliance with a request.".

Insertion of new section 18A into Cap. 140A

3. ***The principal Act is amended by inserting immediately after section 18 the following new section:***

"Confidentiality of request for assistance

18A.(1) A Commonwealth country may require that a request for assistance under this Act be kept confidential except to the extent necessary for its execution.

(2) Where a request for confidentiality under subsection (1) cannot be complied with, the central authority for Barbados shall promptly inform the Commonwealth country.

(3) Where the central authority for Barbados has informed a Commonwealth country that it is unable to comply with a request for confidentiality under subsection (1), the Commonwealth country shall determine whether the request for assistance is to be executed.".

Insertion of new section 20A and 20B into Cap. 140A

4. ***The principal Act is amended by inserting immediately after section 20 the following new sections:***

“Assistance in expediting preservation of computer data

20A.(1) A Commonwealth country may request that the central authority for Barbados obtain an order for the expeditious preservation of data stored in a computer system

(a) located within Barbados; and

(b) in respect of which the country intends to submit a request for mutual assistance in relation to

(i) search or similar access of the data;

(ii) seizure or similar securing of the data; or

(iii) disclosure of the data.

(2) A request for preservation made under subsection (1), shall specify the following:

(a) the authority seeking the preservation;

(b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the stored computer data to be preserved and its relationship to the offence;

(d) any available information identifying the custodian of the stored computer data or the location of the computer system;

(e) the necessity of the preservation; and

(f) that the Commonwealth country intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

(3) Dual criminality shall not be a requirement to comply with a request under subsection (1).

(4) Notwithstanding any provision in this Part, the central authority for Barbados may refuse a request for preservation where

(a) the request concerns an offence of a political character; or

(b) the granting of the request would be contrary to the *Constitution* or would prejudice the security, international relations or any substantial interest relating to national security or other essential public policy of Barbados.

(5) Where in the opinion of the central authority for Barbados a request for preservation may

(a) not ensure the future availability of the data; or

(b) threaten the confidentiality of or prejudice the investigation of the Commonwealth country,

the central authority shall promptly inform the Commonwealth country.

(6) Where the Commonwealth country is informed in accordance with subsection (5), it shall determine whether the request for assistance is to be executed.

(7) The Commissioner of Police, or any other officer designated by him in writing, may make an *ex parte* application for a preservation order to a Judge or magistrate where

(a) computer data, including traffic data, stored in a computer system is required for the purposes of a criminal investigation; and

(b) there are grounds to believe that the computer data, including traffic data, stored in a computer system is particularly vulnerable to loss or modification.

(8) Where the Commissioner of Police satisfies a Judge or magistrate on the basis of the *ex parte* application made under subsection (7), the

Judge or magistrate may make an order requiring the person in control of the computer system to

(a) ensure that the computer data specified in the order be preserved for a period of up to 90 days;

(b) maintain the integrity of the computer data for a period of up to 90 days; and

(c) keep confidential any information or action relating to the preservation order.

(9) Where the Commissioner of Police makes an *ex parte* application for an extension of a preservation order, a Judge or magistrate may extend the preservation order beyond the 90 day period for a further period of up to 90 days.

(10) For the purposes of this section,

"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function;

"computer system" means a device or a group of inter-connected or related devices, one or more of which, pursuant to a programme, facilitates communication, performs automatic processing of data or any other function.

Assistance in expediting disclosure of preserved traffic data

20B.(1) Where in the execution of a request made under section 20A, Barbados discovers that a service provider in another country was involved in the transmission of the communication, Barbados shall expeditiously disclose to the Commonwealth country

(a) a sufficient amount of traffic data to identify that service provider; and

(b) the path through which the communication was transmitted.

(2) Notwithstanding subsection (1), Barbados may refuse to disclose traffic data where

(a) the request concerns an offence of a political character;

(b) the granting of the request would be contrary to the *Constitution* or would prejudice the security, international relations or any substantial interest relating to national security or other essential public policy of Barbados.".

Amendment of section 29 of Cap. 140A

5. ***Section 29 of the principal Act is amended in subsection (1)***

(a) ***in paragraph (a) by deleting the word "and" appearing immediately after the word "matters;";***

(b) ***by inserting immediately after paragraph (b), the following paragraph:***

"*(c)* to any country which is party to the Budapest Convention on Cybercrime.".

Insertion of new section 34A into Cap. 140A

6. ***The principal Act is amended by inserting the following new section immediately after section 34:***

"Spontaneous information

34A.(1) Subject to any enactment relating to mutual assistance, the central authority may, without a request, forward information obtained

within the framework of its investigations to a country if the disclosure of such information is likely to

(a) assist the receiving country in initiating or carrying out an investigation or proceedings concerning criminal offences; or

(b) lead to a request for co-operation by that country.

(2) Notwithstanding subsection (1), the central authority may request, that prior to providing such information, it be kept confidential or only used subject to conditions.

(3) Where the receiving country is unable to comply with a request made under subsection (2), it shall notify the central authority which shall determine whether the information should nevertheless be provided.

(4) Where the receiving country accepts the information subject to the conditions, it shall be bound by them.”.

Read three times and passed the House of Assembly this day of , 2024.

Speaker

Read three times and passed the Senate this day of , 2024.

President

WRITTEN SUBMISSIONS

Niel Harper <niel@nielharper.com> 4/12/2024 12:10 PM

Submission to the Joint Select Committee (JSC) - Cybercrime Bill

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Dear Clerk of Parliament,

Kindly see attached my submission to the Joint Select Committee, including key areas where improvements are required.

Key points addressed are as follows:

- Conditions and safeguards
- Protection of personal data
- Data security & security incident response
- Maintaining data access records
- Transparency and notice
- Judicial and non-judicial remedies
- Oversight

I am also attaching my curriculum vitae (CV) which provides evidence of my background and experience in the areas of law, cybercrime, cybersecurity, privacy & data protection, and law enforcement.

I am also requesting the opportunity to present orally to the JSC.

Can you please confirm receipt of my submission?

Regards,

Niel Harper
Corporate Governance & Cyber Risk
Mobile: +45 305 157 63
Email: niel@nielharper.com
Twitter: @noaharper

- Feedback on the Cybercrime Bill (Niel Harper).pdf (176 KB)
- CV - JSC.pdf (265 KB)

Niel Harper

Phone number: (+49) 17635392981 **Email address:** niel@nielharper.com **Website:** https://nielharper.com

ABOUT ME

Award-winning, results-focused Digital Trust executive leveraging strategic vision and communication skills to influence C-level decision-making while driving innovative risk-based solutions that enhance business capabilities in complex, global organizations. 20 years of leadership experience with demonstrated competencies in corporate governance, Internet law & policy, cyber risk management, privacy program implementation, digital transformation, internal audit, risk oversight, financial oversight, and developing high-performance, geographically diverse teams.

WORK EXPERIENCE

Cybersecurity Expert

EU CyberNet [10/01/2024 – Current]

City: Taliin | **Country:** Estonia

- Participate in unique assignments in different locations around the world in the role of consultant, trainer, or speaker.
- Contribute to cyber capacity building initiatives and provide expertise to the European Union's efforts in partner countries.
- Engage in expert discussions with other experts in the community on various cybersecurity-related issues (e.g., quantum computing, security in satellites, generative AI, cybersecurity in healthcare, etc.).

Independent Management Advisory Committee (IMAC)

ITU [01/01/2024 – Current]

City: Geneva | **Country:** Switzerland

- The IMAC serves in an expert advisory capacity and assists the Council and the Secretary-General in fulfilling their oversight responsibilities, including ensuring the effectiveness of the internal control systems, risk management and governance processes in place at the International Telecommunications Union (ITU).
- Advise the Council on the staffing, resources and performance of the internal audit function and the appropriateness of the independence of the internal audit function in reviewing the scope of internal audit plans and work programmes.
- Advise the Council on the scope and approach of the external auditor's work by highlighting emerging risks from the external auditor's reports, reviewing the adequacy of the management response to the observations and recommendations issued and assisting in avoiding any overlaps between internal and external audit.

Chief Information Security Officer & Data Protection Officer

Doodle [03/01/2022 – Current]

City: Berlin | **Country:** Germany

- Doodle is a leading online scheduling cloud-based service with approximately 30 million users on a monthly basis. The company is part of the TX Group and has staff across physical offices in Zurich (headquarters), Berlin, and Belgrade.
- Developed the organization's information security strategy, focusing on enterprise resilience and collaborative risk governance, and deepening partnerships with key functions such as People Operations, Customer Support, Engineering, Finance, Product, and Growth.
- Implement key capabilities across asset management, incident management, threat intelligence, vulnerability management, identity and access management, vendor risk management, CI/CD security, and others.
- Serve as the company's Data Protection Officer (DPO), leading privacy compliance activities covering multiple jurisdictions (e.g., GDPR, ePrivacy, CCPA, etc.).
- Member of the Enterprise Risk Committee (ERC), tasked with overseeing the complex risk universe of the business.
- Completed SOC 2 Type II audits with zero exceptions and achieved MSP Cyber Verify Level 3 certification.
- Recognized as one of the ***Cyber Security Hub Top 25 Cyber Security Leaders for 2024***.

Technical Expert - Digital Equity Accelerator

Aspen Institute [01/05/2023 – Current]

City: Washington D.C. | **Country:** United States

- Consult and advise organizations through their growth, impact, programming, and professional development.
- Serve as a “technical expert” on technology management, cybersecurity, and privacy.

- Provide consultations, coaching and advice to staff of funded not-for-profit organizations and NGOs that are accelerating digital inclusion (on an as-needed basis) related to my area/topic of expertise.
- Report on all meetings through provided reporting system.
- Key organizations include Dignity for Children (Malaysia), Digify Africa (South Africa), ECubed (South Africa), and Startup Lab MX (Mexico), among others.

Professional Standards Working Group

UK Cyber Security Council [15/02/2023 – Current]

City: London | **Country:** United Kingdom

- Contribute to the widening of community participation within the cyber security profession.
- Shape recommendations for the UK professional standards regime for the cyber security profession following pilot programmes.
- Raise awareness of cyber security specialisms across the industry.
- Collaborate with core council working groups to enhance standards of practice.
- Define professional levels for the cyber security profession in the United Kingdom.

Board Director & Chair, Innovation & Technology Committee

ISACA [04/06/2021 – Current]

City: Schaumburg | **Country:** United States

- Represent and protect the interests of the Information Systems Audit & Control Association's (ISACA) stakeholders, including members, chapters, and partners.
- Support the development of the organization's policies, strategising ways to meet enterprise goals, ensuring that operations abide by relevant laws and regulations and making sure that any decisions or actions align with the interests of all stakeholders.
- ***Chair, Innovation & Technology Committee*** tasked with assisting the Board in guiding, supporting, and challenging actions being taken by management in relation to competitive innovation.
- Serve on the ***Audit Committee (previously Vice-Chair)*** providing oversight of financial reporting, the audit process, the company's system of internal controls and regulatory compliance.

Team Leader/Key Expert, Cybersecurity & Digital Policy

European Commission [07/08/2017 – Current]

City: Brussels | **Country:** Belgium

- Lead or participate in European Commission funded projects in multiple countries in collaboration with key agencies and projects, including the European External Action Service (EEAS), Europol, ENISA, INTPA, Eurojust, EU Cyber Direct, and Cyber4Dev, among others.
- Develop national cybersecurity assessments and roadmaps for EU partner countries.
- Define and coordinate the delivery of cyber capacity building activities in Asia, Gulf States, and the Pacific Islands.
- Perform mid-term evaluations on key projects related to cyber diplomacy, cybercrime prevention, ICT standardisation, privacy & data protection, and digital cooperation.

Chief Information Security Officer (Advisory)

Bemol [10/06/2017 – Current]

City: Manaus | **Country:** Brazil

- Serve as an an advisor to the President and Board of Directors on matters related to IT risk management, cybersecurity, and privacy/data protection.
- Conduct ongoing cybersecurity maturity assessments, looking across people, process and technology and considering risk levels and business impact.
- Develop, monitor, and adjust as needed the business' multi-year strategic roadmap to enhance privacy and cybersecurity capabilities and deliver process improvements, including addressing key risk and compliance priorities and staffing requirements to support executive-level resourcing and investment planning.
- Perform assurance to ensure that recommendations are implemented in an adequate, effective and sustainable manner.

Expert in Cybersecurity, Data Policy, and Risk & Resilience
World Economic Forum [27/02/2017 – Current]

City: Geneva | **Country:** Switzerland

- The Forum's Expert Network brings together leading experts from academia, business, government, international organizations, civil society, the arts, and the media committed to improving the state of the world by helping to shape the global agenda.
- Participate in expert discussions, organize around capacity building initiatives, and engage with existing Forum projects, events and research.
- Serve on the ***Cyber Risk & Corporate Governance Working Group*** with key executives from Hewlett-Packard Enterprise (HPE), Palo Alto Networks, S&P Global, Microsoft, Tech Mahindra, and others where we are focused on fostering leaders' awareness, supporting a community of cyber-aware leaders to champion cybersecurity as an organizational priority, and developing the tools necessary for leaders to govern these new risks.

IT Risk & Compliance Principal
Canonical [16/11/2020 – 10/05/2022]

City: London | **Country:** United Kingdom

- Led the alignment and maintenance of the organization's privacy and cybersecurity processes, policies and technologies in compliance with industry frameworks.
- Completed attestations/certifications for SOC 2 Type II, MSP Cloud Verify, and O-TTPS.
- Executed compliance audits and remediation projects within established control areas, and in collaboration with key teams such as Information Systems, Product Engineering, Application Services, Device Enablement, and Cloud Development.
- Responsible for privacy engineering to address key regulatory requirements (e.g., GDPR, CCPA, ePrivacy Directive, etc.).

Special Advisor on Cybercrime Prevention
Regional Security System [09/11/2020 – 18/03/2022]

City: Paragon | **Country:** Barbados

- Provided expert guidance, oversight and strategic/tactical leadership to enhance cooperation among law enforcement and military to support Member States in preventing and combating cybercrime.
- Key areas of focus included cyber capacity building, digital forensics & access to electronic evidence (e-evidence), cyber incident response, and cyber crime investigation.

Chief Information Security Officer
UNOPS [01/02/2019 – 18/02/2022]

City: Copenhagen | **Country:** Denmark

- Built and delivered from scratch the United Nations Office for Project Services' (UNOPS) comprehensive, strategic enterprise cybersecurity, privacy and IT risk management programs across 120+ countries.
- Led, developed and mentored a global team of 45 full-time employees (FTEs) and consultants.
- Served on the ***IT Steering Committee*** and ***Data Governance Board*** of the organization and on the ***United Nations Information Security Special Interest Group (UNISSIG)***.
- Recipient of the ***ISACA Technology for Humanity Award*** and the ***International Security Journal Security and Resilience Award***.

Senior Consultant, Privacy & Data Protection
Deloitte Consulting [10/02/2021 – 08/12/2021]

City: Bridgetown | **Country:** Barbados

- Provided independent consultancy services to interpret different regulations and assess the effectiveness of privacy controls at customers.
- Oversaw the management of all project elements including risk assessment, data-flow mapping, review of in-scope systems, gap analysis of policies and procedures, technology integration, training, and guidance for future compliance audits.
- Prepared underlying materials, led/participated in client workshops, and drafted/delivered final reports to customers.

Chief Information Officer & Director, Integrated Information Systems (IIS)
CARICOM Secretariat [01/10/2018 – 30/09/2019]

City: Georgetown | **Country:** Guyana

- Established the Secretariat's digital transformation strategy and developed a detailed 5-year technology roadmap in alignment with organizational goals, and in support of overall Member State priorities.
- Led the successful delivery of enterprise IT initiatives, developed and initiated a multi-year training plan, and introduced key policies, standards and guidelines.
- Developed an IT risk management framework and cybersecurity program to address key risks associated with delivering the technology roadmap.

Director, Cyber-Policy Capacity Building
Internet Society [09/04/2012 – 01/03/2019]

City: Reston | **Country:** United States

- I was recruited to establish and mature a best-in-class capacity building program that prepared a new generation to succeed as leaders in Internet technology, policy, and business.
- With financial and in-kind support from organizations such as Google, Afilias, NBCUniversal, Verizon, Microsoft, and Verisign, delivered training to 75,000+ persons from more than 100 countries through moderated online courses, face-to-face training, self-paced tutorials, fellowships, and leadership programs.
- The portfolio of activities covered key topics such as cybersecurity, privacy & data protection, Internet governance & policy, managing online identity, cybercrime prevention, telecoms regulation, secure Internet routing (MANRS), Domain Name System Security Extensions (DNSSEC), and Messaging, Malware and Mobile Anti-Abuse.
- Recognized by the World Economic Forum as a ***Global Shaper*** and a ***Young Global Leader***.

Chief Information Officer
Bermuda Commercial Bank [19/11/2014 – 24/06/2016]

City: Hamilton | **Country:** Bermuda

- The Bank recruited me to spearhead their digital transformation strategy of the group, leading the implementation of key solutions to deliver on-demand scaling, cost reductions, omni-channel customer engagement, manage cyber risk, and adapt to emerging regulatory demands.
- Deployed new capabilities for enterprise cloud, core banking, Internet and mobile banking, data warehouse and business intelligence, AML/KYC,
- Restructured the IT organization, recruiting and developing expertise in IT infrastructure, information security, application support, enterprise architecture, data governance, and IT service desk.
- Managed an annual CAPEX budget of USD$2.5M+ and OPEX budget of USD$5M+.

Head, Network & Security Engineering
CIBC FirstCaribbean International Bank [18/08/2008 – 06/04/2012]

City: Bridgetown | **Country:** Barbados

- Led the strategic, tactical and operational aspects of network and security engineering.
- Delivered more than 30 capabilities including core routing, WAN acceleration, next generation firewalls, network admission control (NAC), MPLS/Metro-E, unified communications call centre, IP telephony, telepresence, and SIEM, among others.
- Direct reports included the team leads for network infrastructure, network security, unified communications, and network architecture.
- Served on the ***Change Advisory Board*** and ***Technical Architecture Committee*** of the organisation.
- Managed an annual CAPEX budget of USD$6M+ and OPEX budget of USD$32M+.

Senior Audit Manager, Technology & Operations
CIBC FirstCaribbean International Bank [12/06/2006 – 15/08/2008]

City: Bridgetown | **Country:** Barbados

- Strengthened the business' control environment and overall technology risk and cybersecurity posture by leading more engaged and collaborative audit coverage for the Technology, Operations and Change Management business units.
- Successfully led key audit engagements such as Data Centre Operations, Information Security Management, Business Continuity Management, Treasury Operations, Wealth Management, and Visa PIN Security, among others.
- Served on the ***Operations and Technology Risk Committee*** of the business.

Manager, Internal & ICT Audit
Telem Group [09/01/2006 – 31/01/2007]

City: Philipsburg | **Country:** Netherlands Antilles

- Developed, led, and executed the overall audit approach for providing independent and objective assurance and consulting services designed to improve the effectiveness and efficiency of the Sint Maarten Telecommunications Group of Companies (Telem Group) operations in Sint Maarten, Curacao, Saba, St. Eustatius, and Dominican Republic.
- Oversaw the end-to-end delivery of financial, operational, regulatory, technology, and project-related audits.

Technical Operations Manager
AT&T Wireless [03/11/2003 – 21/11/2005]

City: Guaynabo | **Country:** Puerto Rico

- Led all operational aspects of AT&T Wireless' 2.5G (GPRS) and 2.75G (EDGE) mobile network, including data centre operations, facilities management, physical security, network security, field operations, switch operations, network optimisation, and staffing/recruitment, all towards optimising key processes and technology.
- Managed an annual CAPEX budget of USD$2.5M+ and OPEX budget of USD$18M+.

EDUCATION AND TRAINING

Master of Laws (LLM), Internet Law & Policy
University of Strathclyde

City: Glasgow | **Country:** United Kingdom

- Specialisation in Cybercrime, Privacy, and National Security

Master of Business Administration (MBA)
University of Leicester

City: Leicester | **Country:** United Kingdom

Postgraduate Diploma (PgD), Telecoms Regulation & Policy
University of the West Indies

City: St. Augustine | **Country:** Trinidad and Tobago

Diploma, Business Information Systems
Algonquin College of Applied Arts & Technology

City: Ottawa | **Country:** Canada

NACD Directorship Certification
National Association of Corporate Directors (NACD)

City: Washington D.C. | **Country:** United States

Executive Education, Strategies for Sustainability
Stanford University

City: Stanford | **Country:** United States

Executive Education, Cybersecurity Leadership & Strategy
Florida International University

City: Miami | **Country:** United States

Executive Education, Smart Cities
Nanyang Technological University (NTU)

Country: Singapore

Executive Education, Transformational Leadership
University of Oxford

City: Oxford | **Country:** United Kingdom

Certificate, Fintech Law & Policy
Duke University

City: Durham | **Country:** United States

Certificate, Sports Facilities Management
Barça Innovation Hub Universitas

City: Barcelona | **Country:** Spain

Certificate, Digital Transformation Strategy
Boston University

City: Boston | **Country:** United States

Certified Data Privacy Solutions Engineer (CDPSE)
Information Systems Audit and Control Association

City: Schaumburg | **Country:** United States

Certified in Risk and Information Systems Control (CRISC)
Information Systems Audit and Control Association

City: Schaumburg | **Country:** United States

Incorporated Engineer (IEng)
UK Engineering Council

City: London | **Country:** United Kingdom

Certified Information Systems Security Professional (CISSP)
(ISC)²

City: Clearwater | **Country:** United States

Certified Information Systems Auditor (CISA)
Information Systems Audit and Control Association

City: Schaumburg | **Country:** United States

US Foreign Corrupt Practices Act (FCPA)
Thomson Reuters

City: Toronto | **Country:** Canada

SWIFT Customer Security Controls Framework v2024
Society for Worldwide Interbank Financial Telecommunication (SWIFT)

City: La Hulpe | **Country:** Belgium

PART II – PROHIBITED CONDUCT

Illegal access

Part II (4) (1-2) is far too broad in its scope and can implicate innocent or well meaning individuals such as cybersecurity professionals, researchers, activists, and whistleblowers. It's even more problematic where judicial officers aren't trained to understand how to distinguish criminality from activities that serve the public interest, protect organizations, or advance the cybersecurity profession.

Certain guidance should be included with the legislation to distinguish between acceptable and criminal behaviours. *****

For example, the European Union (EU) General Data Protection Regulations (GDPR) includes ***172 recitals*** – also known as preamble – that provides context and explains the reasons for the regulations. There was also an ***explanatory memorandum*** that provided further details on the proposed legislation.

Misuse of devices

Part II (9) (a-b) There are a number of dual use programmes and applications which can be and are used for both legitimate testing and protection of computer systems and conversely for malicious intent. There should be language here which acknowledges such and removes criminality in cases of ethical hacking for instance.

Disclosure of access codes

Part II (11) (1) There are several legitimate reasons for sharing access codes or credentials without authority, and this alone should not be illegal. The qualifier for criminality should be when the individual knowingly or has reason to believe that it is likely to cause loss, damage or injury to any person or property.

Critical information infrastructure system

Part II (12) (1) The list of critical information infrastructure (CII) systems is too limited in scope. A broader list should be published as an appendix or guidance note when the act is proclaimed (e.g., financial services, water utility, transportation, healthcare, hospitality, etc.). This should not be vague or left up to interpretation.

Note: Complementary critical infrastructure (CI) protection legislation is needed to ensure that:

- There is a legal framework or a mechanism to identify operators of critical information infrastructure.
- Operators of critical (information) infrastructure are required to assess and manage cyber risks and/or implement cybersecurity measures.

- Public sector organizations are required to assess and manage cyber risks and/or implement cybersecurity measures.
- A competent authority has been designated and allocated powers to supervise the implementation of cyber/information security measures.

Malicious communications

Part II (19) (3) This is deeply problematic and can be used to stifle freedom of expression or valuable public commentary. It can also be leveraged to prevent criticisms of politicians/public personalities or for the purpose of political persecution. This same vague language exists in the Computer Misuse Act 2005, and has been improperly used for the same abuses identified. There must be safeguards and/or independent supervision in place to ensure that such vague clauses are not abused. This applies to several other elements of this Bill. **

Cyber bullying

Part II (20) (1) – Same as the previous comment.

Cyber terrorism

Part II (21) (1-2) This is too limited in scope and should include any use of computer systems for terrorism or organized crime. It should also include preparatory acts for terrorism or organized crimes (these are not the criminal activities themselves but the actions that facilitate or lead up to them).

PART III – INVESTIGATION AND ENFORCEMENT

Search and seizure

Part III (23) (1-2) gives law enforcement excessively broad powers when it comes to confiscation and access to computer systems (including smaller form factors such as tablets and mobile phones). As per the Budapest Convention, and international best practives, these types of powers require safeguards and protections, including but not limited to independent and effective oversight functions.

Safeguards and protections can include independent tribunals, appellate courts, arbitration procedures, specialised judicial branches, data protection legislation, robust data security controls, and transparency notices. The Data Protection Act, if it were properly enforced and the Data Protection Commissioner wasn't politically captured, would also be one of the safeguards.

These conditions and safeguards will protect against human rights violations such as unfair targeting by poorly trained and/or politically biased judges and magistrates, confiscation and access to individuals' devices without established legal basis, stifling the voices of political rivals or digital activists, disproportionate interception and monitoring of online communications, revenge arrests, cyber stalking by law

enforcement officers of rivals or romantic partners, undue blocking or takedowns of websites, rampant and unregulated use of spyware by law enforcement, extended retention and processing of personal data without legal basis, and other related misdeeds.

Assisting a police officer

Part III (24) (1-5) Some of the provisions in this section are concerning and can be used to force individuals to grant access to their personal devices, especially in the event that the grounds for disclosure have not been met. Again, this requires independent and effective oversight functions, and the oath of a police officer shouldn't be enough to obtain a warrant that grants such far reaching powers.

Production of data for criminal proceedings

Part III (26) (1) This gives law enforcement excessively broad and intrusive surveillance powers when it comes to intercepting Internet communications, compelling service providers to handover subscriber data and Internet activity, and other potentially disproportionate collection or interception of online communications. These types of powers require independent and effective oversight functions. Again, the oath of a police officer shouldn't be enough to obtain a warrant that allows for such intrusive acts.

Preservation of data for criminal proceedings

Part III (28) (1-3) There is no discussion of the conditions and safeguards for adequate protection of human rights and liberties when collecting and storing (preservation) data for criminal proceedings. This includes maintaining the "chain of custody", protection of personal data in line with the Data Protection Act, handling of sensitive data, retention periods, adequate security measures, automated decisions (e.g., use of AI), sharing personal or sensitive data with third-parties, records of how data is accessed and used, etc. The provisions should also include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

Safeguards in this instance should also include strong data security and privacy controls for evidence collected and stored by law enforcement to support court cases. What we ***DO NOT*** *want is* content from someone's computer, laptop, and mobile phone or their location data and Internet usage activities *being accessed by all and sundry and shared with unauthorised third parties or altered to unfairly prejudice a court case or violate the privacy rights of citizens. Furthermore, we want to protect against instances where data can be deleted that prevents criminals from being brought to justice.*

The 'chain of custody' is of critical importance in forensics (including digital forensics). This is the paper or digital trail, or the sequential documentation of physical or electronic evidence. It indicates the collection, sequence of control, transfer, and analysis of forensic information. If the chain of custody cannot be verified, then evidence should not

be admissible in court. Government needs to provide assurances that digital evidence cannot be tampered with or shared with unauthorised parties. This is done by maintaining detailed records of who has accessed the data, who has used the data, and with whom the data has been shared.

According to the Data Protection Act and in line with the Budapest Convention, the Government of Barbados needs to have processes in place to provide individuals whose personal data they have collected in relation to the Cybercrime Bill with details of this data and the legal basis for processing it. The process should also allow the person to exercise their rights to correction, amendment, erasure or anonymisation, restriction of processing, or blocking of the processing of their data.

General observations – Part III

Part III (Investigation and enforcement) is missing key provisions related to:

- Joint investigations or joint investigation teams
- Expert witness testimony by video conferencing
- Emergency mutual assistance (which is different to expedited disclosure)

ALIGNMENT WITH THE BUDAPEST CONVENTION

2nd Protocol of the Budapest Convention

It is clear that the Cybercrime Bill was patterned after the Council of Europe's (CoE) Budapest Convention 1st Protocol, which has been deemed as outdated or deficient for several reasons. The 2nd Protocol of the Budapest Convention was ratified on 12 May 2022, which addressed several of the challenges, issues, and criticisms from cyber law experts, privacy professionals, and human rights advocates. The drafters of this Bill do not appear to have integrated the substantive updates from the 2nd Protocol. So it looks like the government is essentially looking to enact legislation that is outdated and not in step with current technology developments or evolving jurisprudence.

***** *Training of judicial officers, especially with regards to technology law and privacy law, is a major problem in the country. Because these specialist areas of law are emerging, there is poor understanding of the issues by magistrates, judges, prosecutors, etc. and limited case law to refer to locally or in other regional jurisdictions. Consequently, many rulings / decisions have flawed bases, and individuals are often under- or over-penalised.*

****** *The Budapest Convention, on which the Cybercrime Bill is based has an accompanying 60-page* ***explanatory report*** *that specifies the additional checks and balances and rule of law-based environment that countries like Barbados should have underpinning their cybercrime legislation.*

The Government of Barbados needs to be transparent with citizens about how their personal data which is processed in relation to the Cybercrime Bill is protected. This includes publishing general or public notices on the legal basis for processing, retention

periods for the data, who the data is being shared with (e.g., international police organizations, foreign law enforcement, professionals / consultants working with law enforcement, etc.), and what redress is available to individuals with regards to misuse and abuse of their personal data.

If someone is not guilty of a crime or is no longer being investigated in relation to a criminal matter, law enforcement has no legal basis for keeping their data, and should delete it. If a legal basis remains, this needs to be formally explained in detail to the individual. This includes any data captured related to content from someone's computer, laptop, and mobile phone or their location data and Internet usage activities.

If the Government of Barbados refuses to allow individuals to exercise their right to privacy in line with the rule of law (including the Data Protection Act), there should be an oversight body that they can appeal to, including an arbitration court with decisions which are binding.

Prepared by: Niel Harper, LLM, MBA, PgD, IEng, CISA, CRISC, CDPSE, CISSP
Date: 12 April 2024

C2

Steven Williams <steven@dataprivacy.bb> 4/18/2024 6:54 AM

Submission of Responses to Criticisms of the Barbados CyberCrime Bill

To parliamentbarbados@caribsurf.com

Dear Select Subcommittee,

I am writing to submit my response to some of the criticisms that have been raised regarding t Barbados CyberCrime Bill. As the IT specialist who played a role in the draft architecture of the and having been involved in the adaptation of the Budapest Convention on Cybercrime to our national context, I believe it is essential to address these concerns constructively.

Enclosed with this email, you will find a document outlining my perspectives on the criticized sections of the bill. They reflect a balanced view, emphasizing the need for the bill to navigate complexities of cybercrime legislation while protecting individual rights and fostering innovatio

While I fully support the bill and its objectives, I also recognize the importance of the review process you are undertaking. It is my hope that my submission will contribute valuable insights your deliberations, helping to refine and strengthen the proposed legislation.

I am available for any further clarification or to participate in discussions should you find it necessary.

Thank you for considering my submission. I look forward to your feedback and the opportunity contribute to the evolution of this critical piece of legislation.

Best regards,

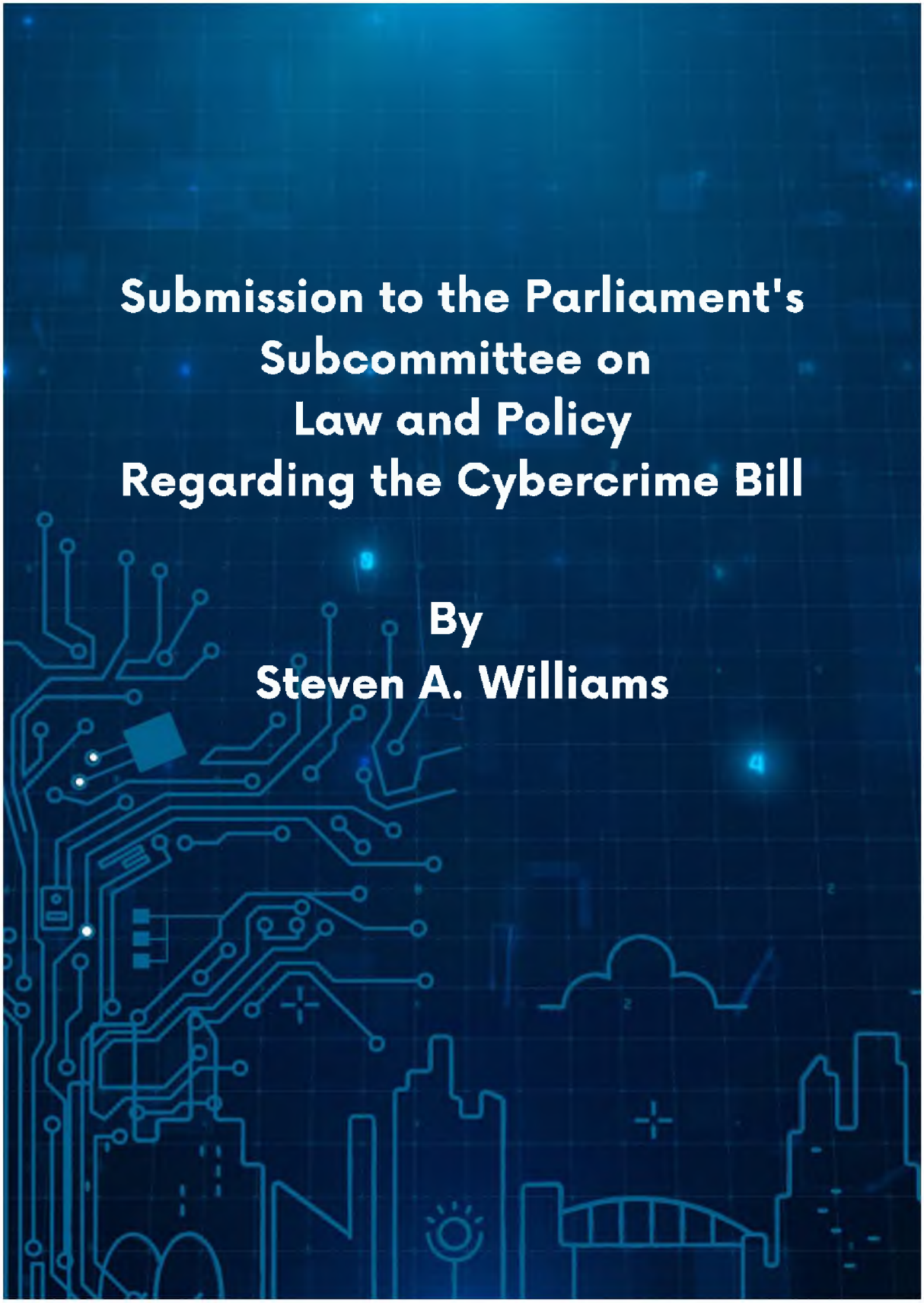
Steven A. Williams, MBA, CCISO, CDPO
Principal Consultant
Data Privacy and Management Advisory Services

Email: dpo@dataprivacy.bb
Phone: 246.233.0090

- Cybercrime Bill submission 2024.pdf (569 KB)

Submission to the Parliament's Subcommittee on Law and Policy Regarding the Cybercrime Bill

By
Steven A. Williams



To Whom it May Concern

I am honoured to present this submission, which outlines my evaluation of the public criticisms of the Barbados Cybercrime Bill. This document aims to foster a nuanced understanding of those specific provisions of the Bill, addressing concerns raised by various stakeholders while offering possible insight to strike a balanced and effective approach to cybercrime legislation.

The digital age has ushered in unprecedented challenges, necessitating a robust legal framework to combat cyber threats while safeguarding individual rights and legitimate digital activities. The Barbados Cybercrime Bill represents a commendable effort to confront these challenges head-on, yet it is imperative to consider the perspectives of cybersecurity professionals, privacy advocates, and civil society organizations to refine its provisions.

This submission looks at the critiques and concerns raised regarding specific sections of the Bill, such as illegal access provisions, critical information infrastructure systems, malicious communications, illegal devices, disclosure of access codes, cyber terrorism, and assisting law enforcement officers. Each critique is accompanied by nuanced support or potential enhancements to ensure the Bill's effectiveness.

I sincerely thank the esteemed members of this Subcommittee for the opportunity to present this submission. It is my hope that the insights and recommendations provided will meaningfully contribute to the refinement of the Cybercrime Bill, positioning Barbados as a leader in combating cybercrime while preserving the fundamental rights and freedoms of its citizens in our digital era.

Respectfully,

Steven A. Williams, MBA, CCISO, CDPO
Consultant to the Cybercrime Bill

Table of Contents

Introduction

The Barbados Cybercrime Bill is a comprehensive legislative effort, grounded in the principles of the Budapest Convention on Cybercrime, to confront the multifaceted challenges posed by cybercrime in our modern digital landscape. While this Bill aims to forge a robust legal framework for combating cyber threats, various aspects of its provisions have drawn scrutiny and criticism from various stakeholders. This document examines the critiques and concerns raised regarding specific sections of the proposed legislation, offering my perspective and proposing potential enhancements to strike a balanced and effective approach to cybercrime legislation in Barbados.

Illegal Access Provisions

With respect to Illegal Access Provisions the critique of the Barbados Cybercrime Bill highlights concerns over its broad scope, potentially implicating individuals like cybersecurity professionals, researchers, activists, and whistleblowers. This interpretation fears the misapplication of the law by judicial officers who may not be adept in differentiating between criminality and activities that contribute to public interest or cybersecurity advancement.

To address these concerns comprehensively:

- **Intention and Authority:** It's crucial to distinguish between malicious intent and authorized cybersecurity actions. Professionals and researchers operate under authorization, focusing on enhancing security rather than undermining it. Their activities are not "reckless" but are driven by the intent to secure systems against threats.
- **Professional Conduct and Organizational Responsibility:** Cybersecurity work, inherently professional and ethical, aims at safeguarding systems with minimal disruption. Organizations engage with such professionals to identify and rectify vulnerabilities, relying on their expertise to bolster defences against cyber threats.
- **Activists and Whistleblowers:** While the actions of some whistleblowers may be necessary, cyber activities akin to those by anarchist groups like Anonymous, though not monetarily driven, can be deemed cyber vigilantism or terrorism. Despite potentially benign intentions, the implications of unauthorized access - such as exposing government secrets or compromising business operations - cannot be overlooked. The digital realm should not provide a haven for actions that would be deemed vigilantism and unlawful in the physical world.

- **The Judiciary's Role:** It is imperative for the judiciary to discern the nuances of cyber activities, distinguishing between malicious intent and actions aimed at public interest or security enhancement. This discernment is crucial to uphold the law effectively while recognizing the complex landscape of cyber interactions. The argument that some hackers could be considered activists does not absolve them from the potential harm their actions could cause, such as compromising state secrets or disrupting business operations. Cyber actions, even those without monetary motives, can have significant real-world consequences.
- **Cyber Vigilantism:** The digital equivalent of vigilantism, even when aimed at exposing wrongdoing, poses a challenge to legal and ethical standards. Actions in cyberspace, though seemingly intangible, have tangible impacts on privacy, security, and operational integrity. As such, they must be scrutinized with the same rigor as physical acts of vigilantism, emphasizing the need for lawful and ethical conduct.

In summary, while the Barbados CyberCrime Bill aims to address unauthorized and malicious cyber activities, it also prompts a nuanced understanding of the diverse actors in cyberspace. Recognizing the legitimate roles of digital stakeholders, alongside the imperative to safeguard against cyber vigilantism, highlights the critical balance the law seeks to achieve. Judicial expertise and discernment play vital roles in navigating this balance, ensuring that actions in cyberspace are held to standards that protect both public interest and individual and organizational integrity.

Critical Information Infrastructure System

The critique regarding the definition and scope of critical information infrastructure (CII) within the Barbados CyberCrime Bill underscores the importance of a comprehensive and adaptive approach to identifying and protecting such infrastructures. Given the dynamic nature of cyber threats and the evolving landscape of critical sectors, the feedback suggests an opportunity for enhancement:

- **Broader and Dynamic Listing:** The current list of CIIs, while encompassing key sectors, may benefit from being more expansive to include other critical services such as those within the chemical industry (e.g., paint and textile companies), which rely heavily on digital systems for monitoring and control. Incorporating a broader list through an appendix or guidance note, updated regularly, could ensure inclusivity and relevance over time.

- **Regulatory Flexibility:** However, moving the list of identified critical services from the Bill to binding Regulations associated with the Act could offer greater flexibility. This approach allows for the timely addition as new sectors emerge driven by technology and as societal changes warrant, without necessitating legislative amendments. Delegating authority to a Minister or relevant agency to update this list ensures responsiveness to evolving cyber and infrastructural challenges.
- **Future Legislation and Frameworks:** Acknowledging the need for a more robust legal and regulatory framework surrounding CIIs, future legislation should aim to:
    - Establish clear criteria and mechanisms for identifying operators of critical information infrastructure.
    - Mandate operators of critical infrastructure, including the public sector, to assess, manage cyber risks, and implement comprehensive cybersecurity measures.
    - Designate a competent authority with the necessary powers to oversee and enforce cybersecurity standards and practices, ensuring alignment with international best practices.
- **International Best Practices:** A future cybersecurity bill should emphasize the alignment of Barbados' critical infrastructure protection measures with international best practices. This alignment ensures that Barbados not only protects its national interests but also contributes to the global resilience against evolving cyber threats.

In conclusion, while the CyberCrime Bill's current provisions on CIIs lay a foundational framework for protection, there's room for refinement and expansion. By adopting a more flexible, inclusive, and forward-looking approach, future amendments and legislation can ensure comprehensive and adaptive protection of Barbados' critical information infrastructure, aligning with both national security interests and international cybersecurity standards.

Malicious Communications

The criticism of the CyberCrime Bill, regarding the potential for misuse against freedom of expression and political commentary, highlights the delicate balance between protecting individuals from digital harm and preserving the right to free speech. This section of the Bill addresses the intentional dissemination of false information that could subject individuals to ridicule, contempt, or embarrassment:

- **Intent as a Core Element:** The Bill specifically targets actions undertaken with "malicious intent". This focus on intent is crucial; as it aims to differentiate between harmful acts designed to intimidate, harass, or distress, and the exercise of free speech, including legitimate public discourse and criticism.
- **Judiciary's Role:** It falls upon the judiciary to discern the intent behind the accused's actions, ensuring that the law's application does not unjustly infringe upon free speech. The judiciary's interpretation and application of these provisions must balance the protection of individuals against digital abuse with the safeguarding of free expression.
- **Legal Protections vs. Freedom of Expression:** While recognizing the importance of free speech, it's essential to acknowledge that this freedom comes with responsibility. The law seeks to protect against targeted, harmful behaviours that exploit digital platforms to cause significant distress or harm to individuals. Ensuring digital spaces are safe and respectful does not negate free speech but rather conditions it to prevent abuse.
- **Necessity of Legal Frameworks:** Although no legal system is flawless, and there maybe instances where individuals are unjustly implicated, the existence of robust legal frameworks is vital for addressing and deterring malicious online behaviours. The law's presence underscores a societal commitment to fostering digital environments where safety and respect are paramount, balancing this with the fundamental right to free expression.

In essence, while the Bill's intention is to provide a legal recourse against malicious digital communications, ongoing vigilance is required to ensure it does not inadvertently suppress legitimate free speech. This Bill emphasizes the judiciary's critical role in interpreting the law with discernment, upholding both individual protection and the principles of free expression.

Illegal Devices

The critique of the Barbados Cybercrime Bill's provisions on illegal devices highlights the potential for dual-use devices and applications to be used both for legitimate cybersecurity purposes and malicious intent. It suggests that the law should acknowledge this dual nature and exempt ethical hacking from criminalization.

The law's focus on the intent behind the possession or distribution of potentially harmful tools is key. It specifically targets actions intended for committing an offense, distinguishing between malicious actors and those engaging in legitimate cybersecurity activities:

- **Intent and Purpose:** The legislation addresses the intent behind the use of devices, programs, or data. By focusing on whether these are intended for use in committing an offense, it differentiates between malicious use and legitimate cybersecurity practices, such as ethical hacking.
- **Parliament's Role:** Parliament is responsible for creating laws that provide a clear legal framework, including definitions of cybercrimes and associated penalties. I my view, the drafting the Barbados CyberCrime Bill, Parliament aims to address the nuanced reality of cybersecurity, recognizing the dual-purpose nature of many cybersecurity tools. The inclusion of intent as a key factor in defining illegal use of devices reflects Parliament's understanding of the complexity of cyber activities and its attempt to legislate in a way that criminalizes malicious intent while protecting legitimate cybersecurity efforts.
- **Judiciary's Role:** The judiciary's responsibility is to interpret and apply these laws to individual cases, considering the intent and circumstances surrounding each accused's actions. This involves discerning whether actions under scrutiny were genuinely aimed at committing an offense or were part of legitimate cybersecurity practices. The judiciary's role in uncovering the motivations behind actions ensures that ethical hacking and similar activities are not unjustly penalized under the broad provisions of the law.
- **Legislative and Judicial Balance:** This distinction between the roles of Parliament and the judiciary underscores the law's precision in targeting cybercrime. While Parliament provides the legal framework, the judiciary interprets this framework in specific contexts, ensuring that the application of the law does not hinder legitimate cybersecurity activities.

In essence, the Barbados CyberCrime Bill's section on illegal devices is designed to penalize malicious intent while safeguarding legitimate cybersecurity activities. The law emphasizes intent, aligning with the judiciary's role in discerning the motivations behind the accused's actions, and reflects Parliament's commitment to creating a nuanced legal framework that addresses the complexities of the digital age.

Disclosure of Access Codes

The criticism regarding the Barbados Cybercrime Bill's provisions on unauthorized disclosure of access codes highlights the nuances surrounding the sharing of credentials. The law aims to penalize individuals who share passwords, access codes, or other means of accessing computer systems or data without proper authorization, especially when such actions are intended for unlawful gain or are likely to cause damage. However, the concern that legitimate instances of sharing access codes could fall under this criminalization deserves attention:

- **Legitimate Sharing vs. Criminal Intent:** It's essential to distinguish between the sharing of access codes in a benign context and actions intended to facilitate unauthorized or malicious access. For instance, sharing a Netflix password with family members or an Amazon account with a friend is commonplace and typically does not result in harm. These actions lack malicious intent and are unlikely to cause signficant loss, damage, or injury, which should be the threshold for criminality.

Enhanced Scenario 1: Corporate Espionage

- Imagine an employee who, driven by grievances or monetary incentives, discloses corporate login credentials to a competitor. This act not only breaches trust but potentially jeopardizes sensitive data and corporate integrity, qualifying as a clear instance of criminal intent deserving of the penalties outlined in the bill.

Enhanced Scenario 2: Malicious Data Breach

- Consider a scenario where an individual intentionally shares access codes to a government database with a hacker group, knowing it could lead to data theft or public exposure of sensitive information. Such an act, motivated by malice or ideological reasons, could result in significant harm and should be unequivocally criminalized.
- **Distinction Between Criminal and Civil Cases:** The law might benefit from clarifying distinctions between criminal actions and those better addressed as civil matters. Unauthorized sharing of passwords that leads to violations of service terms, without further harm, might be more appropriately handled through civil remedies. Conversely, sharing that endangers personal, corporate, or national security warrants criminal sanctions.

- **Proposal for Amendment:** Incorporating language that specifically addresses the intent behind unauthorized disclosure—emphasizing the likelihood of causing loss, damage, or injury—could refine the law. This amendment would help protect individuals engaging in harmless sharing from criminal charges to what may more be a civil matter, while still targeting genuinely malicious activities.

In conclusion, while the Barbados CyberCrime Bill seeks to mitigate risks associated with unauthorized access, a more nuanced approach distinguishing between different contexts and intentions of sharing access codes can enhance its fairness and effectiveness. By refining the law to focus on malicious intent and potential for harm, it becomes possible to balance the protection of digital assets with the realities of modern digital interactions.

Cyber Terrorism

The criticism of the Barbados Cybercrime Bill's provision on Cyber Terrorism for being too narrow in scope raises significant points about what is terrorism in the digital age. The current definition may not fully encapsulate the breadth of activities and actions associated with cyber terrorism:

- **Evolving Nature of Terrorism:** Cyber terrorism represents a departure from traditional terrorism, chiefly in its methods and impact. The absence of direct physical violence in cyber terrorism distinguishes it from traditional forms, focusing instead on compromising digital infrastructures to cause disruption, financial loss, or indirect physical consequences such as power outages.
- **Broader Impact Spectrum:** The primary targets and victims of cyber terrorism are the digital frameworks and data upon which modern societies rely. The potential for substantial indirect harm through such attacks necessitates a broader understanding of terrorism within the cyber realm.
- **Need for Specificity in Legislation:** Given these distinctions, the definition of terrorism as outlined in the Anti-Terrorism Act, Cap. 158, may not adequately cover the spectrum of activities that constitute cyber terrorism. There's a compelling argument for expanding the definition within the CyberCrime Bill to include preparatory acts and the use of computer systems for terrorism or organized crime, even when these acts don't culminate in traditional terrorist activities.
- **Adapting Definitions for Cyber Context:** To accurately address the threat of cyber terrorism, it may be beneficial to introduce a definition specific to the cyber context. This definition should account for the unique motivations, intents, and methods of cyber terrorists, including preparatory acts that facilitate larger cyber-terrorist schemes.

In response to the criticism, it's clear that while the current provisions aim to tackle cyber terrorism, there exists a need for a more comprehensive and nuanced approach. This includes specifically defining cyber terrorism within the CyberCrime Bill to reflect its distinct characteristics and the wide array of activities it encompasses. Such an adaptation ensures that legislation remains effective and responsive to the evolving landscape of cyber threats.

Assisting a Police Officer

The criticism of Section 24 of the Barbados CyberCrime Bill, which outlines the obligations of individuals to assist police officers in accessing computer systems under a warrant, highlights crucial privacy concerns and the potential for misuse in encroaching on personal digital spaces. Particularly, the worry centers on forcing individuals to unlock personal devices without adequate safeguards against self-incrimination:

- **Safeguards Against Self-Incrimination:** It is essential that the Bill explicitly includes protections to prevent the misuse of disclosed information for self-incrimination. While cooperation with law enforcement is crucial, the Bill must ensure that individuals are not compelled to provide evidence against themselves, except under clearly defined conditions.
- **Judicial Oversight:** Any request for such disclosure should be rigorously scrutinized and approved by a judicial authority or a designated senior official. This step is critical to balance law enforcement needs with individual rights, ensuring that the power to demand access to personal devices is exercised judiciously and with respect to the principles of justice and privacy.
- **Exceptions for National Security and Serious Crimes:** While safeguards are necessary, exceptions may be warranted in cases involving national security, or the prevention and detection of serious crimes or terrorism. Even so, these exceptions should be narrowly defined and applied sparingly, to prevent broad or arbitrary application.
- **Need for Independent Oversight:** Independent oversight mechanisms should be established or strengthened to review the application and execution of warrants requiring individuals to assist in accessing computer data. This oversight serves as a check against potential abuse, ensuring that law enforcement powers are not exercised without appropriate cause or justification.

Considering these concerns, the legislation should be amended to incorporate clear safeguards against self-incrimination and ensure that any compelled assistance in accessing computer systems is subject to stringent judicial oversight and independent review. By doing so, the Bill can achieve its objectives of combating cybercrime while upholding the rights and privacy of individuals.

Conclusion

The effectiveness of the Barbados CyberCrime Bill hinges on the ability of the judiciary to discern the intent behind the actions of defendants in cybercrime cases. Many of the Bill's provisions, such as those addressing illegal access, malicious communications, illegal devices, and the disclosure of access codes, require a nuanced understanding of the motivations and purposes underlying the alleged criminal acts.

To ensure the fair and just application of these provisions, it is imperative that Barbados establishes a judicial system with the requisite structure, resources, and training to manage cybercrime cases effectively.

Furthermore, when enacting the CyberCrime Bill, it will be crucial to implement strong Regulations to strengthen areas that have been identified as potential gaps or needing more clarity. One key area is providing a robust framework for identifying critical infrastructure services that need heightened cybersecurity protection. The ability to dynamically update the list of recognized critical sectors through binding regulations will allow the law to remain agile and responsive to evolving threats and technologies.

The judiciary must also be equipped with the necessary tools and expertise to distinguish between malicious intent and legitimate cybersecurity activities, such as ethical hacking and security research. This discernment is crucial to prevent the unintended criminalization of professionals and individuals acting in good faith to enhance digital security and serve the public interest.

Ultimately, the success of the CyberCrime Bill rests not only on its provisions but also on the capacity of the judicial system to interpret and apply those provisions with wisdom, impartiality, and a deep understanding of the complexities inherent in the digital realm. A well-structured and trained judiciary, bolstered by agile regulations that can adapt to changing cyber threats, will be the cornerstone of Barbados' efforts to combat cybercrime while upholding the principles of justice and the rule of law.

BCEN Barbados <bcen246@gmail.com> 4/22/2024 2:12 PM

Memoranda- Cybercrime Bill

To parliamentbarbados@caribsurf.com

To: Clerk of Parliament,
Parliament of Barbados,
Parliament Buildings,
Trafalgar Street, Bridgetown.

Dear Sir

Attached please find official correspondence from the Barbados Consume Empowerment Network (BCEN) with recommendations for consideration on the Cybercrime Bill, 2024 and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024.

Kindly acknowledge receipt of this email and attachment.

Regards
Maureen Holder

- Official Document for Clerk of Parliament- CYBER CRIME BILL.docx (333 KB)

BARBADOS CONSUMER EMPOWERMENT NETWORK

C/o Mailing address: Maureen Holder No12
Warrens Crescent, St Thomas

Bcen246@gmail.com
moeholder@hotmail.com
(246) 427-2023/8323372

Date: 22/04/2024

To: Clerk of Parliament,
Parliament of Barbados,
Parliament Buildings,
Trafalgar Street,
Bridgetown.

MEMORANDA

Re: Inclusion of Digital Finance Provisions in the Cybercrime Bill for Consumer Protection

On behalf of the **Barbados Consumer Empowerment Network** (BCEN), I am writing to express our strong support for the inclusion of protection provisions for consumers using digital financial platforms in the anticipated revised Cybercrime Bill. As an organization dedicated to advocating for consumer rights and empowerment, we believe that there should be explicit provisions included in the Bill to protect and safeguard the welfare of consumers in this digital age. BCEN recognizes that the proliferation of digital financial services and the increasing reliance on online transactions have brought about significant benefits for consumers, e.g. convenience, accessibility, and efficiency. However, we also recognize that along with such benefits are inherent threats from cybercriminals who seek to exploit any vulnerabilities in digital platforms via fraud, theft, and other financial crimes.

After careful review of the Cybercrime Bill, (that is currently in a state of revision) BCEN is of the view that it indirectly facilitates consumers, but it does not explicitly focus on digital finance protection for consumers. Neither does the bill focuses on redress or penalties for digital financial crimes against consumers. Therefore, BCEN believes that given the increasing prevalence of cyber threats targeting consumers in an era of digital financial services or (FinTech), it is essential for the Barbados Cybercrime Bill to include digital finance protection for consumers as a key component of its legislative framework.

The ITU and the World Bank's "Digital Regulation Platform" has a separate chapter on consumer affairs which highlights several important issues related to consumer protection such as: **(a)** consumer rights in the digital context; **(b)** good practices in consumer support; **(c)** digital consumer rights (consumer consultation); **(d)** consumer requirements from regulators; **(e)** dispute resolution; **(f)** and good practices in consumer outreach and education. The **Barbados Fair-Trading Commission's Consumer Protection Act** ***[CAP. 326D]*** does not comprehensively address digital financial services as a particular area of focus for consumers.

Therefore, BCEN believes that there should be mechanisms included in the Cybercrime Bill to facilitate the reporting of digital financial crimes and providing support and assistance to victims, as well as ensuring that there is swift and effective redress through legal and regulatory channels for consumers; especially consumers with special needs or have a disability. In other words, BCEN is of the view that there should be specific provisions addressing consumer rights, fraud prevention, and dispute resolution in digital transactions. Such mechanisms and provisions should be supported by clear procedures for reporting digital financial cyber crimes and investigating complaints. The intention behind such provisions would be to ensure that consumers operating in the digital financial space have access to fair and effective justice. BCEN interprets this to mean that included in the Cybercrime Bill should be legislation that empowers individuals to act against perpetrators of financial cybercrimes, as well as allow them to seek appropriate remedies for any damages they incur. Enforcing penalties against perpetrators of financial cybercrimes sends a strong message that such behaviour will not be tolerated. It will also serve as a deterrent to potential offenders and help to prevent future instances.

BCEN believes that by incorporating these provisions into the Cybercrime Bill, Barbados can demonstrate its commitment to consumer protection, foster trust in digital financial services, and create a safer and more secure environment for consumers to undertake online transactions. We believe that proactive legislative action in this regard is essential for safeguarding the interests and rights of consumers in our increasingly digitized society. We trust that our recommendations will be given due consideration in the drafting and enactment of the Cybercrime Bill, and we look forward to collaborating with relevant stakeholders to advance consumer-centric policies and initiatives in Barbados. ***[Cont.]***

Thank you for your attention to this matter. Should you require any further information or assistance, please do not hesitate to contact us.

Sincerely,

BARBADOS CONSUMER EMPOWERMENT NETWORK

Maureen P. Holder
EXECUTIVE DIRECTOR

David Weekes <david.weekes@icloud.com> 4/22/2024 5:20 PM

Invitation to make a Presentation pertaining to the Cybersecurity Bill

To clerk@barbadosparliament.com • parliamentbarbados@caribsurf.com Copy tdw@westcoastlegal.bb • cidhdenuncias@oas.org • margaret.kimberley@blackagendareport.com • Ken Farrell <farrello@gmail.com> • carolmartindale@nationnews.com • tips@cnn.com • watchdog@bbc.co.uk • press.int@aljazeera.net • editorial@nationnews.com • advocate@sunbeach.net • editorial@gleanerjm.com • newsroom@guardian.co.tt • peterharris@barbadostoday.bb • sandydeane@barbadostoday.bb • supporter@nasguard.com • news@barbadosadvocate.com • news@jamaicaobserver.com • admin@stvincenttimes.com • news@stluciastar.com • stabroeknews@stabroeknews.com • info@thevincentian.com • news@newsday.co.tt

Dear Sir

I am a Barbadian, living in exile, one who has especial interest in **this CyberSecurity Bill given potential victimization by this and/or any future Government of Barbados.**

Indeed, having been **firebombed at my Barbados home**, because of my digital campaign about **my Denial of my Right to Due Process**, for 17 years, my reading of your already concluded CyberSecurity bill inclines me to contemplate a few things, chief amongst which is the degree that citizens, and residents, **may be affected, and explicitly targeted, under your 2024 Bill.**

As a Third Sector community leader of what was one of the 3rd largest NGOs in Barbados, and a digital activist with over 20 years of experience in this field, I believe that I can contribute to the discussion.

I write specifically requesting **to make an Oral Presentation** in keeping with the Government of Barbados' April 8 2024 Press Release that invites such presentations.

I began this email by stating that I live in exile but, as a member of the Barbadian diaspora that Barbados Prime Minister Mia Mottley ostensibly embraces, I can but hope that she as UN Secretary General aspirant, (the leading post that represents global citizenry,) might ensure **that Zoom presentations are afforded to all Barbados' Diaspora Citizens for this seminal Human Rights topic - Freedom of Speech.**

Looking forward to hearing from you

David Weekes

Hugh B. Shepherd <punchathome@hotmail.com> 4/22/2024 8:02 PM

I am sharing 'Cybercrime Act 2024 (3)' with you

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Get Outlook for Android

- Cybercrime Act 2024 (3).docx (19 KB)

Dear Sirs

There are two sections, of the Cybercrime Act 2024 that are in contravention of the Universal Declaration of Human Rights (UDHR) and/or the International Human Rights Law that concern me, and should either be amended or omitted from the act. These are:

1. Section 19 (3) "A person who intentionally uses a computer system to disseminate any image or words, not caring whether they are true or false, and causes or is likely to cause or subject a person to ridicule, contempt, or embarrassment is guilty of an offence and is liable on summary conviction to a fine of $70,000 or to imprisonment for a term of 7 years or to both. "

This contravenes freedom of expression which is an integral part of human rights. In fact, the right to freedom of expression has been recognised as a human right in the Universal Declaration of Human Rights and the International Human Rights Law by the United Nations. It states, "Everyone shall have the right to hold opinions without interference" and "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". and

2. Section 19 (5) "***The defences of truth***, comment, triviality and privilege, ***whether absolute or qualified***, provided for under the Defamation Act, Cap. 199 ***shall extend to a prosecution under subsection (3).***"

This is also a breach of human rights. International Human Rights Law provides that while individuals should have the right to a legal remedy for defamation, this right must be balanced with the equally protected right to freedom of opinion and expression. In general, to ensure that domestic defamation law adequately balances individuals' right to protect their reputation with freedom of expression and the press, it entails:

Providing for truth to be a valid defence (i.e., demonstrating that the content of the defamatory statement is true),

Recognising reasonable publication on matters of public concern as a valid defence, and

Ensuring that defamation may only be addressed by the legal system as a tort.

Again, sections 19 (3) and 19 (5) either conflict with the Universal Declaration of Human Rights, the International Human Rights, Defamation or any combination of these laws.

I strongly recommend therefore that these concerns be given precedence and careful consideration during your upcoming review.

Kind regards,

Hugh B. Shepherd

Chesterfield St.C Browne <chesbrowne@gmail.com> 4/22/2024 10:43 PM

Submission to the Joint Select Committee of Parliament - Chesterfield Browne

To parliamentbarbados@caribsurf.com

Dear Clerk of Parliament,

Please find attached my written submission for consideration by the Joint Select Committee (Standing) on Governance and Policy Matters (Cybercrime Bill 2024).

In the submission, I state my support for a Cybercrime Bill but outline a number of concerns about the legislative process and content of Cybercrime Bill 2024 and offer recommendations for the committee to consider.

I trust this submission will be helpful to the Committee's deliberations. I am happy to answer any questions the committee may have in writing.

Thank you for your time and consideration.

Sincerely,

CSBrowne
Chesterfield St. C Browne

- CYBERCRIME 2024 SUBMISSION TO JSC.docx (94 KB)

A CRITIQUE OF THE CYBERCRIME BILL 2024

Cybersecurity vs. Civil Liberties: Ensuring a Fair and Effective Cybercrime Bill for Barbados

Submission to the Joint Select Committee (Standing) on Governance and Policy Matters

APRIL 19, 2024

PREPARED BY CHESTERFIELD ST.C BROWNE

I do not wish to make an oral submission.

Mr Chairman, I write to express my views and concerns about Cybercrime Bill 2024.
This document consists of two sections. Section A examines and critiques the process used to reach the committee stage, and Section B examines and critiques sections of the bill that I find problematic.

Section A

At the outset, I posit that a well-drafted Cybercrime is necessary to curb illegal online activities and provide a safer digital landscape for Barbados' citizens and businesses, provided the Bill protects civil liberties. However, I wish to express concern about the content and process of the Cybercrime Bill 2024, which has led to the bill's referral to the Joint Select Committee (Standing) on Governance and Policy Matters. In my opinion, the process deviates from the typical Westminster system flow. I suggest that the Senate could have approached the situation differently:

1. **Identify Concerns and Send the bill Back to the House:**
    - The Senate could have clearly outlined their specific issues with the Bill. It could have involved concerns about privacy rights, limitations on free speech, or a lack of clarity in the legislation.
    - A formal communication could be sent back to the House of Assembly detailing these concerns and recommending amendments.

2. **House of Assembly Considers Amendments:**
    - The House would then review the Senate's concerns and decide on a course of action.
    - They could:
        - Accept the concerns and propose amendments to address them.
        - Reject the concerns and send the Bill back to the Senate unamended, along with a formal explanation for their decision.

3. **Back and Forth or Reaching Consensus:**
    - If the House proposes amendments, the Bill would return to the Senate for consideration.
    - The Senate could then:
        - Accept the amendments and pass the Bill.
        - Reject the amendments and potentially request a conference committee (explained below).
    - This back-and-forth might occur a few times until an agreement is reached.
4. **Joint Select Committee as a Last Resort:**
    - If significant disagreement persists, a conference committee could be formed.
    - This committee would consist of members from the House and Senate tasked with finding a compromise version of the Bill.
    - Their proposed amendments would need approval by both houses before the Bill is finally passed.

Benefits of this Approach:

- Following the steps of the established Westminster system ensures **clarity and transparency** in the legislative process.
- It allows for proper debate and consideration of concerns from both houses.
- The Joint Select Conference Committee would be used as a last resort to provide a mechanism to break deadlocks.

Conclusion to Section A

Involving the Joint Committee at this stage bypasses the back-and-forth communication between the houses, potentially leading to a less transparent and efficient resolution even though there might be the contention that submissions from the public will make a transparent process. The Senate should have focused on clearly communicating their concerns to the House and followed established legislative steps. This would ensure a more transparent and effective process for amending the Cybercrime Bill.

Section B

I now analyse and comment on the sections of the Bill that appear problematic from my perspective.

Section 20 (1) of the Barbados Cybercrime Bill 2024 on cyberbullying does have some areas of vagueness, particularly around the ***exclusions for artistic expression and satire.***

This section defines cyberbullying as intentionally using a computer system to publish, broadcast, or transmit data that meets several criteria, namely - Offensive Pornographic, Indecent, Vulgar, Profane, Obscene, and Menacing character.

According to Section 20(1), It must also be done with the intent to cause harm to another person, such as annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety, and substantial emotional distress.

Concerns – Vagueness of terms:

As a layman, I find some of the terminology used to be vague, with multiple possible interpretations, for example:

- The list of offensive characteristics for data is subjective and open to interpretation. **What one person finds offensive, another might not.**
- The exclusions for artistic expression and satire are not explicitly mentioned, which could lead to confusion.

This vagueness can lead to unintended and undesirable consequences for the citizens of Barbados. These undesired outcomes include but are not limited to:

i. A chilling effect on free speech, as citizens of Barbados might be afraid to express themselves online for fear of prosecution.
ii. Unequal application of the law, depending on the interpretation of "offensive" by law enforcement or the court.

Recommendations:

Regarding this section, I wish to offer the following recommendations

i. Consider including more precise definitions of the offensive characteristics listed in the bill or remove them from the bill.
ii. Explicitly state exemptions for artistic expression, satire, and political commentary as long as they do not meet the other criteria of causing harm or containing pornography.
iii. This would provide more clarity for citizens and reduce the potential for misuse of the law.

A synopsis of Sections 23 to 28 reveals that they extend broad powers of search and seizure without the requisite checks and balances that protect the citizens of Barbados. The extent of the powers is cause for concern. ***We are a people who treasure the freedoms that are enshrined in our constitution.***

- **Section 23** grants police broad search and seizure powers, allowing them to access, copy, and even render inaccessible computer data upon obtaining a warrant.
- **Section 24** compels anyone with knowledge of a computer system or storage medium to assist police with a warrant, including potentially decrypting data.
- **Section 25,** while requiring a list of seized data to be provided, allows for the possibility of withholding information by a police officer or approved person who conducted the search and seizure. This behaviour could prejudice the investigation.
- **Section 26** allows courts to order individuals to submit specified computer data.
- **Sections 27 & 28:** These sections deal with preserving internet traffic data and other computer data for investigations.

Critique of sections 23 – 28

- **The Absence of a Clear Legal Basis for Data Seizures:** The Cybercrime Bill 2024 falls short of providing a clear legal framework outlining the justification for seizing citizens' personal and private data. Relying solely on suspicion to gain a warrant is insufficient grounds for such an intrusion. Just as mere suspicion would not prompt calling the police on John Q Public without evidence of a crime, data seizure should not occur based on speculation or mere suspicion. ***Furthermore, the Bill fails to address situations where malicious actors (hackers and scammers) might plant data on a user's device without their knowledge or consent.***

- **Lack of Expertise:** The Bill lacks a requirement for specific IT or cybersecurity qualifications for police officers handling seized data. This raises concerns about potential mishandling of evidence or data breaches. In the complex digital world of policing, high-level technical skills must be mandatory.

- **Self-Incrimination:** Compelling someone to decrypt a device could be seen as compelling self-incrimination, a potential violation of human rights enshrined in the Barbadian Constitution.
- **Data Corruption:** The Bill is silent on how citizens can be compensated if police actions corrupt or erase their data. Data and information have significant monetary value; our lawmakers must acknowledge this.
- **Limited Oversight:** There is a lack of an independent oversight body to monitor law enforcement's use of these data access powers. This raises concerns about potential abuse of power by law enforcement if no one can provide external oversight.

Recommendations:

It is given that cases will arise where there is the need to access computer systems, for example, in the investigation of paedophilia, computer fraud, and computer hacking. With specific reference to the previous examples, our legislators must ensure that due consideration is given to the following:

- The Bill should mandate IT training for police officers handling digital evidence, ideally within a department staffed by personnel with high-level skills in cryptography and computer forensics.
- Law enforcement should explore alternative methods of obtaining encrypted data, such as seeking legal means to compel cooperation from relevant third-party service providers (e.g., Apple, Microsoft) to access cloud-stored data.
- The Bill should include a straightforward procedure for citizens to seek compensation for data corruption or erasure by police actions.
- An independent body should be established to oversee law enforcement's use of these data access powers.

Conclusion

A well-crafted Cybercrime Bill should strike a balance between protecting citizens from online threats and safeguarding fundamental rights. Good legislation is characterised by clarity, precision, and due process. Vague terms like "*offensive*" can lead to misinterpretations and

unequal application. Similarly, granting law enforcement broad search and seizure powers without proper oversight mechanisms undermines citizen trust and creates opportunities for abuse.

For the Cybercrime Bill to be truly fair, it must uphold Barbadian citizens' right to privacy, freedom of expression, and due process. By incorporating the recommendations outlined above, the Barbadian government can ensure that this Bill effectively combats cybercrime while respecting the core principles of a just society.

Chesterfield St.C Browne <chesbrowne@gmail.com> 4/26/2024 9:39 PM

Third submission to the Joint Select Committee of Parliament - Chesterfield Browne

To parliamentbarbados@caribsurf.com

Dear Clerk of Parliament,

I am attaching my third written submission for consideration by the Joint Select Committee (Standing) on Governance and Policy Matters (Cybercrime Bill 2024).

In the submission, I provide commentary on Deepfake Technology and its potential negative impact on law enforcement, the legal profession, and the court system in the context of the Cybercrime Bill 2024.

I believe that this submission will be helpful to the Committee's deliberations. I do not wish to make an oral presentation, but I am happy to answer any questions the committee may have regarding the commentary in writing.

Thank you for your time and consideration.

Sincerely,

CSBrowne
Chesterfield St. C Browne

- COMMENTARY ON DEEPFAKE TECHNOLOGY.pdf (231 KB)

DEEPFAKE TECHNOLOGY

Unmasking the Legal Implications and Challenges with the Cybercrime Bill 2024 in Mind

SUBMITTED BY: Chesterfield St. C Browne

I do not wish to make an oral presentation.

As the Joint Select Committee (Standing) on the Cybercrime Bill 2024 conducts its review, the looming threat of Deepfake Technology in Cyberspace becomes increasingly significant. Policymakers, legal professionals, and parliamentarians must be made aware of this technology. ***While I am neither an AI expert nor legally trained, my research for a previous submission led me to the subject of deepfake technology. I am confident that this submission will alert those reviewing the Cybercrime Bill by highlighting a significant challenge to our law enforcement and court system.*** In light of the emergence of Deepfake technology in the digital landscape, this commentary serves as a reminder to the Committee about the magnitude of their responsibility in reviewing the Cybercrime Bill.

What is Deepfake Technology?

Deepfake Technology is computer software that uses artificial intelligence to create fake videos or audio recordings of people that look and sound exactly like the real thing. It is like a high-tech version of impersonation or mimicry, where the computer learns to mimic a person's face or voice. For example, it could be used to make a video of a celebrity saying things he or she never actually said or to make a fake phone call that sounds like it is coming from your friend. The technology is called "deepfake" because it uses "deep learning" (a type of artificial intelligence) to make the "fake" content. It is a powerful technology that can also be misused, so it is essential to be aware of it.

The Challenges of Deepfake to the Legal System

This technology presents a significant challenge not only to the legal system and the admissibility of some video and audio evidence in court but also to our overall trust in information and the potential for misuse. ***Imagine a scenario where a Barbadian citizen X is seen on social media making a statement about another citizen Y that, according to the Cybercrime Bill 2024, may cause "annoyance, inconvenience, embarrassment, insult, injury or humiliation".*** The question must now be asked: is it real or fake?[1]

[1] https://www.policechiefmagazine.org/law-enforcement-era-deepfakes/

Deepfake is a powerful and potentially disruptive technology that presents new challenges to law enforcement and necessitates new attention to types of investigations, evidence collection, and court proceedings. Consequently, any legislation relating to the digital space must consider Deepfake's challenges to our legal system. At the policy level, due care must be taken to address the various dimensions of deepfakes and determine what measures and procedures are required to keep pace with this and other emerging technologies.

Implications for Legal Professionals

Deepfake technology poses unique challenges for legal professionals[2]. For law enforcement, it complicates the process of gathering evidence. Once considered solid proof, a video or audio recording may now be questioned for its authenticity. This necessitates the development of new tools and techniques to detect deepfakes.

For prosecutors and defence lawyers, deepfakes introduce a new layer of complexity. They must now consider the possibility that evidence presented in court could be fabricated using deepfake technology. This could lead to wrongful convictions if a deepfake is mistaken for real evidence, or it could enable criminals to escape justice by discrediting genuine evidence as a deepfake.

Court officials and judges must now be educated about deepfake technology and its potential impact on court proceedings. In their work, they will be required to make difficult decisions about the admissibility of video and audio evidence and the standards required to establish its authenticity.

Consider a scenario where a deepfake video is presented as evidence in a court case. The defence argues that the video is a deepfake, while the prosecution maintains it is genuine. Both sides present expert witnesses who offer conflicting opinions.

[2] https://jolt.richmond.edu/2023/11/06/deepfakes-navigating-legal-challenges/

The judge must then decide whether to admit the video as evidence and how much weight to give it in their final decision. This scenario illustrates the complex issues that courts will face in the era of deepfakes.

In conclusion, deepfake technology has far-reaching implications for the legal field[3]. It challenges long-held assumptions about the reliability of video and audio evidence and requires legal professionals to adapt to a rapidly changing technological landscape. As such, ongoing education, research, and policy development[4] will be crucial in addressing the challenges posed by deepfakes.

[3] https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology
[4] https://legaljournal.princeton.edu/the-high-stakes-of-deepfakes-the-growing-necessity-of-federal-legislation-to-regulate-this-rapidly-evolving-technology/

References

Dauer, Frederick. 2022. "Law Enforcement in the Era of Deepfakes." Police Chief Online. June 29. [accessed April 25, 2024]. https://www.policechiefmagazine.org/law-enforcement-era-deepfakes/?ref=cdc285c5f3355599c05402cb647b0694

Hutchinson, Moses. 2023 Deepfakes: Navigating Legal Challenges. Jolt Richmond. [accessed April 25, 2024]. https://jolt.richmond.edu/2023/11/06/deepfakes-navigating-legal-challenges

Riehle, Cornelia. 2022: https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology. Europol report on the criminal use of deepfake technology. Eucrim. May 28. [accessed April 26, 2024].

Quirk, Caroline. 2023. "The High Stakes of Deepfakes: The Growing Necessity of Federal Legislation to Regulate This Rapidly Evolving Technology." The Princeton Journal of Law & Public Policy. June 19. [accessed April 26, 2024]. https://legaljournal.princeton.edu/the-high-stakes-of-deepfakes-the-growing-necessity-of-federal-legislation-to-regulate-this-rapidly-evolving-technology/

Chesterfield St.C Browne <chesbrowne@gmail.com> 4/25/2024 1:36 PM

Submission to the Joint Select Committee of Parliament - Chesterfield Browne

To parliamentbarbados@caribsurf.com

Dear Clerk of Parliament,

Please find attached my written submission for consideration by the Joint Select Committee (Standing) on Governance and Policy Matters (Cybercrime Bill 2024).

In the submission, I state my support for the Cybercrime Bill 2024. However, solid legal frameworks alone are insufficient. I posit that effective oversight mechanisms are equally critical to ensure public trust and the responsible use of law enforcement tools. The attached document highlights the need for the inclusion of a Cybercrime Investigation Oversight Committee (CIOC) in the Cybercrime Bill 2024 to strengthen it.

I trust this submission will be helpful to the Committee's deliberations. I am happy to answer any questions the committee may have in writing.

Thank you for your time and consideration.

—
Sincerely,

CSBrowne
Chesterfield St. C Browne

- ESTABLISHING A CYBERCRIME INVESTIGATION OVERSIGHT COMMITTEE.docx (162 KB)

ENHANCING BARBADOS' CYBERCRIME BILL 2024

The Need for a Cybercrime Investigation Oversight Committee (CIOC)

Abstract

The rise of cybercrime is a global concern, and Barbados is no exception. The Cybercrime Bill 2024 represents a significant step forward in combating cybercrime and safeguarding our citizens in the digital age. However, legal, solid frameworks alone are insufficient. Effective oversight mechanisms are equally critical to ensure public trust and the use of law enforcement tools responsibly. This document highlights the need for the inclusion of a Cybercrime Investigation Oversight Committee (CIOC) to strengthen the Barbadian Cybercrime Bill 2024.

Submitted by - Chesterfield St. C Browne

I do not wish to make an oral submission.

Introduction

The rise of cybercrime is a global concern, and Barbados is no exception. The Cybercrime Bill 2024 represents a significant step forward in combating cybercrime and safeguarding our citizens in the digital age. However, legal, solid frameworks alone are insufficient. Effective oversight mechanisms are equally critical to ensure public trust and the use of law enforcement tools responsibly.

Oversight Concerns and Proposed Solutions

The Bill grants significant powers to law enforcement for collecting, processing, and storing digital data during cybercrime investigations. While these powers are crucial for investigations, their execution raises concerns about potential privacy infringements and misuse. For instance, without proper oversight, there is a risk of critical digital evidence vital to proving innocence being withheld.

The Importance of a Cybercrime Investigation Oversight Committee

To further strengthen the investigation provisions of the Cybercrime Bill 2024, I suggest the establishment of a Cybercrime Investigation Oversight Committee (**CIOC**). This committee would be empowered to review law enforcement procedures, conduct audits, and issue recommendations, thereby safeguarding against the previously mentioned concerns.

The United Kingdom (UK), Australia, and the United States (USA) have oversight committees for cybercrime investigations. In the UK, an Investigatory Powers Commissioner's Office (IPCO) has been appointed under the Investigatory Powers Act 2016. The independent body oversees the UK's investigatory powers exercised by public authorities. Its remit includes oversight of surveillance, interception, and data access powers used in cybercrime investigations.

According to the UK government's website (***https://www.gov.uk***)[1], Home Secretary Amber Rudd stated, "*The Investigatory Powers Act offers a world-leading oversight regime to ensure*

[1] https://www.gov.uk/government/news/investigatory-powers-commissioner-establishes-oversight-regime

the powers the security and intelligence agencies and law enforcement use to investigate crimes and protect the public are used responsibly and proportionately."

The IPCO website ***(https://www.ipco.org.uk/)***[2] explains the commission's role in the following way:

"*At IPCO, we oversee the use of covert investigatory powers by more than* ***six hundred public authorities****, including the UK's intelligence agencies, law enforcement agencies, police, councils, and prisons. This means that we independently review applications from public authorities to use the most intrusive of these powers and check that all the powers are used in accordance with the law. All of this work is overseen by the Investigatory Powers Commissioner. We continually seek to understand new and developing technologies, operations, and legislation to ensure that privacy is protected, safeguards are applied, and individual rights are maintained.*"

In Australia, the Independent National Security Legislation Monitor (INSLM) provides independent oversight of Australia's national security legislation, including laws related to cybercrime investigations. The same applies to the USA and Canada, where similar bodies oversee public authorities' investigative practices to ensure transparency and investigations conducted within the law.

Proposed Amendments to Strengthen the Cybercrime Bill with a CIOC

I propose the following amendments to enhance the Cybercrime Bill by incorporating a robust CIOC with functions that allow for:

1. **Transparency and Accountability (Amendment 1)**: The Bill's features are limited in the areas of transparency and accountability from my layman's perspective. The CIOC should be mandated to issue regular public reports detailing its activities and findings to foster trust and transparency in how law enforcement handles and utilises digital data in their investigations.

[2] https://www.ipco.org.uk/what-we-do/

2. **Data Protection Safeguards (Amendment 2):** There are attempts at safeguarding data in a limited way. The safeguards must be more comprehensive. By empowering the CIOC to conduct independent audits to ensure adherence to data privacy laws and regulations, we can protect citizens' rights and prevent the misuse of personal information.

3. **Improved Practices (Amendment 3):** By enabling the CIOC to function as a collaborative body, the committee can guide law enforcement in implementing best practices for data handling through recommendations and collaboration. This leads to more secure and efficient investigations.

4. **Sunset Provisions (Amendment 4):** Currently, there is no CIOC. If one is established, then by including provisions for periodic review of the CIOC's effectiveness and mandate by an independent body, we can ensure its continued relevance and effectiveness.

5. **Composition and Independence (Amendment 5):** Currently, no CIOC is proposed in the Bill. By defining a transparent process for selecting CIOC members who possess relevant expertise and a proven commitment to data privacy and civil liberties, we can guarantee the independence of the CIOC from undue influence by law enforcement agencies.

Conclusion

The Barbadian government's commitment to a robust cybercrime framework is commendable. By establishing a strong CIOC, Barbados can ensure its cybercrime legislation is effective and upholds data privacy principles and public trust in the digital age. I urge the committee to consider these proposed amendments to benefit our citizens and our country's digital future.

Mac Holder <macholder@yahoo.com> 4/23/2024 3:08 AM

CyberCrime Bill

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Thanks for the opportunity to add my opinion despite the fact the Lower House passed the Bill in its vague and erroneous state. Most reasonable Barbadians, accept the need for modern relevant Cyber Laws to mitigate malicious acts and bad actors. I have suffered at the hands of malicious social media post thanks to the current immunity enjoyed by netizens.

Section 19,20 and 21 needs refining as espoused by Chairman Hon Edmund Hinkson, Senator Gregory Nicholls and the Honorable Ralph Thorne.

As a person, who is concerned about mal administration in the absence of a Freedom of Information Act, sometimes hard questions in the interest of public good must be asked which may be seen as public bad. How do we get transparency in government, accountability and fair play when ITAL and FOIA are both absent? However, with such open statutory definitions of menacing, annoyance, embarrassment, insult, injury needless anxiety, emotional abuse, intimidation etc., reasonable respectful free speech is threatened if the Cyber Bill is accepted in its current form.

Please see the below scenario.

$700M Cahill was a GOB fiasco mired in less than transparent acts by the DLP led administration. The late Dr Denis Lowe was Minister of Environment, and was asked hard questions everyday via Facebook, blogs and the call-in radio. I led the task with deliberate INTENT of seeking full disclosure as director of advocacy of the environmental NGO, The Future Centre Trust. His financial dealings with the Cahill principals, and the leaked signed contract were questioned. Lead to his angry response and that of his colleagues using parliamentary privilege to attack me and FCT from the well of parliament.

What could be my possible defense if the late Dr Denis Lowe claimed annoyance, embarrassment, insult, reputational injury, emotional abuse and intimidation?

What guarantee a magistrate or judge whose hiring is not totally immune from political influence rules without a bias?

Why are there no provisions for warning of first offence rather than summary, and indictable offences?

Laws should not be about making money at the feet of nefarious acts but pivot more towards deterrents and restorative justice.

Finally, Sir David Simmons used Nigeria quite often during his presentation, however Nigeria Cybercrime Law, just imprisoned a young mother for an unfavorable tomato paste review. The police arrested this young mother for saying the tomato paste was too sweet as the owner of the business claimed the comment was injurious to their business. Thus, what checks and balances will be in place to ensure no abuse by police officers or politicians as happens with wiretapping as exposed by a former Police Service Commission.

Kammie Holder

Kammie M Holder,FSS,LUTCF,MBLAS,DOSQ
Solving the problems of others is my talent, and task towards self-actualization!

Donna Every <donnaevery1@gmail.com> 4/24/2024 11:58 AM

Submission on the Cybercrime Bill

To parliamentbarbados@caribsurf.com

I would like to submit the following regarding the Cybercrime bill. My understanding of a cybercrime is:
Crimes related to illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography, and offenses related to copyright and neighboring rights. Therefore my concern is that this bill, as it stands, is not truly focused on cybercrime and could be used to make freedom of speech and freedom of religious beliefs a crime if a writer uses words that may cause "annoyance, embarrassment, insult, emotional distress" etc. These, to my mind, while hurtful, are not criminal offenses and should not be included in this bill. I believe we already have legislation that deals with issues such as libel and slander. I am also generally concerned about the broad definitions given in the lastest slew of legislation seeking to be passed and the room left for interpretation. The political parties may well find themselves before the courts for cybercrimes if this bill is passed in its current form.

Donna Every

Melissa Goddard <goddma@gmail.com> 4/24/2024 3:59 PM

Comments on the Cybercrime Bill (2024) for Joint Select Committee

To parliamentbarbados@caribsurf.com

Attached you will find a copy of my comments on the Cybercrime Bill (2024) for consideration by the Joint Select Committee.

I thank you for your time and attention

Kind regards,
MA Goddard PhD

- Comments on the Cybercrime Bill_MAG.pdf (349 KB)

Citizens have been asked to submit their opinions on the Cybercrime Bill, as it is being reviewed by the Joint Select Committee. But I am dismayed that the Commission seems more inclined to stand in defence of the Bill—to the point of making appeals to emotion and straw man and ad hominem arguments, as well as calling out individual citizens from the protections of the Committee. Rather than doing as it has been challenged: to dispassionately and in an unbiased fashion re-examine the contents of the Bill in light of what is a reasonable and global concern; to factor in the input and recommendations of the valuable resource that is Bajan subject matter experts; to hear and address the voiced desires and concerns of all the citizens our Legislature is supposed to represent; and to make a robust and informed consideration of the full breadth of material—not just a single or handful of sources—that is available for decision-makers facing a similar crossroads of ensuring that there is a clear textual distinction between prosecuting actual crimes, and simply criminalising citizens who fall out-of-favour with ruling powers. At least if this is meant to be a sincere effort by this Committee, and not a showy simulation of the Democratic process.

To come from a place of emotion and personal feeling—rather than logic, established guidance and fair reason is precisely why so many of our citizens fear reprisal and the potential downstream effects of this Bill. Criticism of what is a fairly important piece of legislation, one that will affect the daily lives of any and every Barbadian using the Internet today, cannot be seen as—or met with—a personal or political attack.

That is the very heart of freedom of speech and expression—the ability to speak up, speak out or just grumble without fear of legal action, even when one has a dissenting or unpopular personal or political belief, even if one is considered less respected, educated or of lower standing than those privileged enough to more directly access and influence power and by those holding that power, and even if what you are engaged in is not particularly nice or virtuous. Freedom of speech and freedom of expression are for the rabble and the royal alike, and covers curse and compliment equally. Intentional, for some undefined degree of recklessness or otherwise.

Having someone dislike you because of something they heard or said, or feeling embarrassed or offended because of something posted on the internet is not an adequate benchmark or legal reasoning to limit someone's right to free speech or expression. And is highly inappropriate for the very specific topic that is cybercrime. And if someone who has been around as long as, and who is as credentialed as the head of the Commission himself seems unable to make the distinction between what is an example of a cybercrime under the Bill and what isn't, what is freed or criminal

expression, or what is a personal, professional or political response, then this only underscores the depths of the issues with this Bill.

Indeed, the Committee itself serves as an apt illustration of the confusion raised by the Bill's poor drafting. In his defence of this Bill, the Chairman cited as an example the dissemination and his subsequent receipt of pornography. As the pornography in question was presumably created by a consenting adult and is therefore not currently illegal in Barbados, one might imagine that the source of his "significant distress" was that he personally found it morally objectionable, and experienced some upsetting emotion or embarrassment at its sight. But a personal moral objection or personal upset or embarrassment by a single individual cannot be considered good grounds for prosecution. Or we would criminalise the eating of pork, vulgar dancing in public spaces, and violent horror movies, as certain theocracies do. Someone with ophidiophobia may find snakes "substantially distressing." Simply adding that person to a particularly active herpetology group could be an offence under the Bill. And it shouldn't be.

This may seem as hyperbolic as many have been in their defence of the Cybercrime Bill. But the fact remains that if a well-respected and highly experienced legislator is of the opinion that simply receiving a pornographic image is cause enough to call the police on someone, and falls short of including certain claimed criteria for prosecution in his own example of an action that should qualify for prosecution under this Bill—a Bill which we presume is not meant to also ban all internet adult pornography in Barbados—that alone shows that it allows for a broadness of usage and professional or legal interpretation well beyond the stated intent. He has provided us with clear evidence that the Bill is vague, confusing and that there is risk of misuse and misunderstanding. Quod erat demonstrandum and merci beaucoup, as it were.

All that is being asked of legislators is that this broadness be tightened by better drafting and more precise language. If vaunted experts in the law and cybercrime cannot themselves find consensus with what the Bill actually says and does, and are instead left to squabble back and forth on and present all manner of emotive arguments on what they personally think and believe, then the Bill is demonstrably unclear and must be amended or redrafted with clearer cut and more definitive language. Language that cuts through any confusion and establishes a universal consensus in keeping with current definitions of what cybercrime actually is. Or this poorly drafted Bill should be entirely replaced with legislation that is of the high quality that Barbados deserves. It should not be left open to misinterpretation and potential misuse by those whose objections may be aimed at

policing what are personal moral, political, or religious beliefs and behaviours, rather than using the law as a tool against inarguably harmful, criminal and dangerous acts.

As an aside, I should also mention that a Cybercrime Bill does not and cannot address lying, misinformation or disinformation, and that if there is some vague attempt to criminalise the spreading of any word or picture that one has not taken (some entirely undefined notion of) "caring" to determine the veracity of, this can only serve to criminalise free speech. That's the firm position of current and proven understanding and study. What's more, libel and slander are already covered by other existing legislation.

That this Bill wanders through many very different uses of the internet—from issues of privacy, bullying, terrorism, revenge porn, hacking, libel, disinformation and more—and yet never fully lands on or properly deals with any of them is part and parcel of the problem. It also does not treat with or consider many of the more up-to-date technologies, such as AI. As such, it is woefully outdated, out-of-step and peculiarly uninformed, and therefore worthy of deep amendment, one conducted with the support of an expert panel suitably trained and experienced in these areas.

On that note, I must also make a potentially distressing and embarrassing—but still inarguably true—statement. Namely that any career politician, lawyer or economist who has neither relevant advanced training nor appropriately in-depth experience is in a position to cogently rebut any technical criticism outside that wheelhouse if that criticism is made by a subject-matter expert speaking well within theirs. They lack the required level of understanding to identify what can be subtle flaws, to navigate the nuances and jargon of what are very complex topics, are likely unaware of established understandings, consensuses and hard-won historical lessons, and are not informed enough to separate motivated flattery and empty pontification from fact. They are more likely to grossly overestimate their grasp of the material and competence (*Light et al. Sci. Adv. (2022)*), undermine stated aims at the most fundamental levels due to confusion or lack of information, and cannot even know what they do not know, despite however much bluster, name dropping, arrogance or practised oration is used to disguise or compensate for that fact. A degree in economics or law does not allow someone whose last formal training in STEM was at the secondary level—and in the last century—the ability to formulate a proper assessment of an expert comment, far less make a useful response to it without some equivalently and appropriately qualified assistance and support. (And this is typically why legislation of this nature is done with the very transparent help of some sort of expert advisory panel. Before and during—rather than after—drafting. This constantly repeated refrain of "we have no obligation to take expert recommendations" by those

whose knowledge base is superficial and performative at best is not in keeping with good governance or standard international practice towards progressive and functional democracy. That the Electorate is expected to accept it as the norm is inexcusable. We have expensively educated a full two or three generations of Barbadians. Tap into—and stop dismissing—that investment just because it is politically inconvenient.)

Technical comments on a technical Bill demand a certain level of technical understanding. This is a harsh but unavoidable reality. It is therefore incredibly irresponsible for any such unqualified political person to dismiss expert comments on the back of little more than posturing and without the proper deliberation they owe to the Electorate, and to therefore risk pushing through what could be harmful, anti-democratic or unenforceable and therefore useless legislation.

Nevertheless, we can all agree that revenge porn, cyberterrorism, defamation and libel can and should all be criminalised under some form of legislation. (Even if it is not this legislation, and perhaps not all under the same piece of legislation.) These reprehensible behaviours all have well established, legal definitions, ones that can be used without fear of accidentally criminalising innocent people, making public disagreement, satire or social media use a crime, and further bogging down our already beleaguered and sluggish judiciary with additional cases whenever someone's feelings are hurt or sense of propriety is repeatedly offended.

So I remain perplexed as to why there is this stubborn insistence on keeping the Bill exactly as inexact as it is, and not even compromising on the need for some level of amendment or tightening up of the language. Why not bring it into line with the stated intentions and international standards for battling cybercrime, while protecting Bajan freedoms by definitively erasing potential gaps and confusion? Is it ego? Ignorance? Or is the intention of the Bill truly to leave the door ajar just enough that it might allow for some prosecution beyond the promised limits?

It should also be mentioned that defenders of the Bill who, with scant regard and without support, dismiss concerns about the misuse of such legislation to threaten and silence dissenting opinion also ignore Barbados' long history of empowered people doing precisely that. A history we claim to celebrate every National Heroes Day. Many of those we now call nation builders faced the kinds of legal challenges in their pursuit of Bajan Civil Rights that this Bill seeks to reinstate albeit updated for the 2020s.

Samuel Jackman Prescod was jailed for the often acerbic and impolite criticisms of the unjust and bigoted Bajan Legislature he penned for the Liberal. The Herald was a critical voice for the Barbadian

Labouring underclass until repeated lawsuits and accusations of libel pushed it into bankruptcy and silence, leading to the exile of its editor Clennell Wickham. Clement Payne was brought before the courts for making false statements, charged, and actually won his case. But he still was ultimately deported because of that prosecution—an act which triggered the Riots. Simply because he organised meetings where he railed against and baldly criticised the ruling plantocracy. And even quite recently, we have the threatening of the public with legal letters, a threat that could be construed by those inclined to a less than charitable way of thinking as a way of silencing calls for further investigation into and some legal action on the collection, use and declaration of funds by elected officials and Ministers in the interests of combating even the appearance of corruption.

Dissent against established authority—and rude, repeated, and reckless dissent at that—is at the heart and history of Barbadian identity and civil liberty. And the mere threat of legal action against that—against those who already lack privilege, just because they hurt the feelings of the 'wrong' privileged person—has long been used in Barbados as a weapon to subjugate our people. This is what our history books and newspapers tell us. A position that says never mind the mess, just leave it to the law courts seeks not to bring Barbados into the 21st century, but instead pushes us right back into the darkest most unequal days of our past.

Because it also must be pointed out that the speech of those in power remains protected, despite this Bill. Elected officials retain the right to desecrate House and Senate floors by attacking private citizens and making whatever denigrating comments they desire, whether they are true or false. These negative and sometimes outright offensive remarks are often boosted and circulated both off and online by official and journalistic channels, which is something the average Barbadian can realistically do very little about. Elected officials and even members of this Committee can call out individual citizens as they like, and besmirch personal and professional reputations without any fear of reprisal, reprimand or rebuttal, all for an official and now electronic record. The average citizen has no such protection and no equivalent platform. The vagueness inherent to the Cybercrime Bill as currently passed therefore draws a clear and dividing line between The Two Barbadoses, with those empowered to speak and have their words spread as they want and without thought towards the harm they cause on one side, and leaving the average citizen silenced into submission on the other.

Social media provides one of the few platforms where each and every Bajan can openly voice their concerns and opinions, raise awareness of what are often shared fears, and educate each other in the face of what is all-too-often an opaque, vague and inarticulate governing class. We would not

even be here today discussing something as important as Bajan freedom of speech without it. Yet this Bill threatens to make even these meagre spaces unsafe for any kind of discourse, and particularly hostile to any mention that does not meet Government pre-approval or some privileged notion of cautious or respectable conduct.

Where else can Bajans go to raise awareness about the potential paying of £3 million by the Barbados Government to a descendant of a prominent family of enslavers for the acquisition of their plantation, to push repeatedly until leadership is finally shamed into some response? (And yes, shame and embarrassment are one of the few tools left to the otherwise disempowered masses. Or is naming and shaming to be restricted to Houses, Committees and political platforms?) Where can we share our fears about the steady conversion of precious agricultural land for more house spots built on water courses, or the demolition of Heritage districts and property in the pursuit of Brutalist architecture, seaview-obscuring hotels and US dollars? Where can we talk about the shifting and potential hiding away of those who are unhoused or who are mentally ill because tourists might find the sight of them unseemly? How else can we teach each other the language and complexities of the Edifice Complex, crony capitalism, or helicopter science? Are we meant to limit ourselves to penning quiet letters to Ministers, hoping that we have tempered our complaints with enough pandering to get a sitdown and a handshake before we are shuffled off with yet another canned response? If we are not ignored outright, as is the habit in this time of the now 5 Day Wonder?

Should we be prosecuted because a politician or Minister could find any talk akin to my comment today "reckless," "embarrassing" or "significantly distressing" or accuse me of not demonstrating enough "caring?" Or are we allowed, as truly democratic citizens, to speak aloud, freely and in the open, and without fear that we might find ourselves in court for simply exercising that right?

A democracy that stifles disagreement—that does not care to clearly delineate the separation between an unpleasant statement and an actual crime—is no democracy at all. We have already lived as the underclass in such a state and should have no desire to return to it.

Barbadians are repeatedly asked to trust and believe, and to take on faith that those who hold the reins of power and who control our judiciary act—and will always act—with good intentions. That the road paved by these good intentions is a heavenly one. But it is a theocracy that stands on faith, not democracy. A democracy, if it is to be functional, must stand on legislation. And we are called, as "strict guardians" and "firm craftsmen of our fate" to protect that democracy through legislation that doesn't simply hope and pray for the best of current governance, but instead strictly and firmly ensures that our Republic, our citizens and our rights remain protected well into the future, and

even if those who are less than scrupulous manage to find their way into positions of power. A lesson our neighbours in the United States are learning the hard way. To support legislation that is weak and open to overly broad use and interpretation is to support a weakening of our democracy and its essential freedoms.

All our citizens—whether we like, respect or agree with them, and whether or not what they say makes people like us a little less—have a right to a platform and a voice. A right that should clearly and without confusion be reflected in every relevant piece of our legislation. We should not in any way risk the prosecution of or even unintentionally intimidate citizens whose only crime is holding a dissenting opinion, failing to follow respectability politics, or not being entirely enamoured with a Government nearly 70% of the eligible Electorate did not vote for in the last Election. And we should be able to put aside ego, party loyalty, personal feelings and petty behaviours as we do so. Indeed we must ensure that, at all times and at every opportunity, none of those things very subjective things has a legislated influence on our Republic.

I thank the Committee for their time and in the spirit of the Right Hon. Errol Barrow would like to make it known that I will also be sharing both the contents of this comment and the nature of any response as widely as I am able, as currently remains my right. I urge all who hear these words to stand on the right side of Barbadian history. To act not only in the heat of current-day political contention and tribalism, or under the convenient sway of acceptable mediocrity, but with a fair and informed mind towards the proper preservation of our Democratic future and its freedoms, and in accordance with the recommendations of all our brightest, most accomplished experts. We must truly, mindfully, actively and selflessly move forward as a nation, not seek to rebrand and relaunch the injustices of the past in our efforts to shield personal egos or political reputations from fair condemnation.

As such, we should significantly amend, redraft or completely withdraw The Cybercrime Bill and replace it with better-drafted legislation.

M.A. Goddard PhD

Judy M Driscoll <judymdriscoll2@gmail.com> 4/24/2024 5:14 PM

Cybercrime Bill 2024

To parliamentbarbados@caribsurf.com

To whom it may concern

"19(3) A person who intentionally uses a computer system to disseminate any image or words, not caring whether they are true or false, and causes or is likely to cause or subject a person to ridicule, contempt or embarrassment, is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

...

I think that this portion of the bill is making something that is legal (saying a true story, for example, which causes embarrassment to a person in a group) into something illegal because it's now being said on a computer or smart device.

There should be an amendment to this.

Regards
Judy Driscoll

Hugh Greene <greenehugh50@gmx.com> 4/24/2024 8:04 PM

To parliamentbarbados@caribsurf.com

Dear Sir/Madam,

To Whom it may concerned,

My name is Hugh Patrick Greene. I am an Electrician, Computer Technician and Indpendent Software Developer for Windows and Linux Operating Systems. I have written various apps and is a contributor for an opensource game development software named Enigma-dev, under the handle 'hpg678'.

I am writing to state strongly on my refusal on supporting the present draft of the proposed Cyber Bill 2024. As I listened to the live broadcast that was streamed on Youtube, i cannot deny that the 'language' on certain aspects pertaining to 'offences' is in itself too vague and can open itself to misuse and abuse. As one senator used said example of a person calling another fat, could that person be charged even if the statement is true. Regulating 'feelings', 'distress', and that which is abstract in nature is both dangerous and impossible to quantify.

According to Wikipedia :->
"cybercrime covers a wide range of criminal activities that are carried out using digital devices and/or networks. These crimes involve the use of technology to commit fraud, identity theft, data breaches, computer viruses, scams, and expanded upon in other malicious acts." It goes on to state :->
'In 2000, the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders placed cyber crimes into five categories: unauthorized access, damage to computer data or programs, sabotage to hinder the functioning of a computer system or network, unauthorized interception of data within a system or network, and computer espionage.'

Throughout the presentation I found it interesting that as members of the commitee stated/admitted that they were not 'well acqainted' with the aspects of social media and the like, yet they were 'confident' enough to endorse/propose a bill on a topic they know nothing about. Did they consult with computer professionals, psychologists or psychiatrists? Or are they so arrogant to believe they need not to?

Mr. David Simmons put forward an example. One which can be dismissed as one lacking security on their and can be solved by using an AdBlock and/or going into the settings of the device and turning on Parental Controls which negates/blocks such things as porn or unwanted ads to appear on one's phone. No need to draft a Cyber Bill or use that as an example.

In closing, I hope that more time is taken with the focus being on what is best for us as a Bajan society without any war, heinous crimes and signs of terrorism. A peaceful nation where the average person concerns are to live in peace as they struggle to survive every day. They should not let another culture and their laws place a heavy influence on ourselves. Our law-makers and as such, should enforce/draft laws that fits Barbados society and not go the route of 'monkey see, monkey do.'

This is not who we are!

Theresa Annel <ca930730@gmail.com> 4/24/2024 8:10 PM

Cybercrime Bill

To parliamentbarbados@caribsurf.com

To Whom It May Concern

I find it highly offensive the idea of my ideas, thoughts and words are to be controlled/censored because someone's feeling is hurt or they feel embarrassed because of my right to express myself. Furthermore this bill needs to be clearer and more specific in its language.
In an effort to keep it short, I will end here, but I have other concerns on how this will affect innocent children who may not be able to fully understand it's content and normally do things that aren't clearly mentioned in the Bill.

Thank you for your time and have a good day.

Margaret G <margaretgit@hotmail.com> 4/24/2024 8:12 PM

Cyber Crime Bill

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

I am not happy with this bill because I feel my rights will be taken away and my freedom of speech as well .
If this bill passes will we still be living in a democratic country.

v hoy <vhoy09@gmail.com> 4/24/2024 10:25 PM

Re: Cybercrime Bill

To parliamentbarbados@caribsurf.com

I apologize, I didn't sign my name. My name is Valerie Hoyte and I do not support parts of this bill.

On Wed, Apr 24, 2024, 10:22 PM v hoy <vhoy09@gmail.com> wrote:

> Good evening Everyone,
>
> The Cybercrime bill effects free speech. I am aware that free speech is conditional.There are areas of this bill that should've been socialized in a town hall meeting or should be on the ballot for voters to consider. Creating an environment that stops people from speaking up by invoking fear is problematic. Making a bill so broad that one can interpret it in anyway is bad. Living in an idealistic world is just that, we protect the young and the elderly, but we can't stiffle words . It is the cybercrime bill today , what would it be tomorrow?

Mervin Marius <greedygunther@gmail.com> 4/24/2024 10:37 PM

Objection to Cybercrime Bill 2024 in its current form

To parliamentbarbados@caribsurf.com

Esteemed Panel,The Bill in its present form will present a challenge to Churches and Religious Organisations in the exercise of their right to worship and religious instruction,a right enshrined the Constitition of Barbados,,the Supreme Law.The Christian Bible contains portions that can be deemed offensive to certain groups in our society.Homosexuals can take offense to the portion in the Bible that says Homosexuality is an abomination to God.>The LGBTQ+ group can claim hate speech effectively threatening our right to quote from our religious documents.Any Law that contradicts the Constitution may be deemed null and void .End of Submission.Thank you.

Peter Thompson <peterlawrencethompson@gmail.com> 4/25/2024 6:33 AM

Cybercrime Bill is a perversion of fundamental justice

To parliamentbarbados@caribsurf.com

Sir David Simmons, chairman of the Law Reform Commission, made a presentation to this Joint Select Committee in which he referred to my public assertion that the Barbados government's **Cybercrime Bill, 2023** criminalises the freedom of speech of Barbadians. He sought to discredit my assertions but failed miserably. To the contrary, Sir David's oration serves to reinforce the fact that this Cybercime Bill contains a substantive attack on freedom of expression in Barbados.

Sir David asserted that the Law Reform Commission went to great lengths to say that the defences of truth, comment, triviality, and privilege provided under the **Defamation Act Cap.199 (1997)** shall extend to the bill, but he completely neglected to justify why the **Cybercrime Bill** criminalises activities that are completely legal under the **Defamation Act Cap. 199**. He further said that Barbadians were free to transmit data as long as it did not defame others ***or*** cause any of the distresses listed in the bill. This made it clear that the Bill criminalises free expression which is not defamation. I hope that he isn't going to imply that that Act is deficient, because it was Sir David himself that put it through Parliament when he was Attorney-General in 1997.

It is a perversion of fundamental justice that lawful speech in person suddenly becomes a criminal act when expressed online.

To be specific, the vague and deeply problematic uses of the terms "intimidates a person". "embarrassment", "annoyance", and "emotional distress", are nowhere to be found in the **Defamation Act Cap. 199**. It is utterly intolerable for you to subject my lawful speech, which does not breach the **Defamation Act Cap. 199,** to criminal prosecution under the **Cybercrime Bill 2023** part II 20.(1) simply because I choose to express it online.

The Budapest Convention, and by extension the **Cybercrime Bill 2023**, are designed to address the following:
1) Substantive law - Definition of criminal offenses such as illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography, and offenses related to copyright and neighboring rights.
2) Procedural law - Collection of evidence to successfully prosecute the defined criminal offenses.
3) International cooperation on matters related to cybercrimes (closely related to #2)

The Cybercrime Bill goes well beyond these parameters.

The **Defamation Act Cap. 199** already provides clear law to regulate the limits of freedom of expression for Barbadians. It is intolerable that the Cybercrime Bill should seek to impose new limits on speaking out or being vocal about social and political matters. It is utterly unacceptable that speech which does not breach the **Defamation Act Cap. 199** might be subjected to criminal prosecution under the Cybercrime Bill simply because it is expressed online.

Peter Lawrence Thompson MBA, CFRE (Ret.)
Career Success Coach

"...the function of freedom is to free somebody else"
---Toni Morrison

Peter Earle <peterearlebb@yahoo.co.uk> 4/25/2024 9:58 AM

Objection to the Cybercrime Bill

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Sir David Simmons

Chairman,

Law Reform Commission

Dear Sir David Simmons,

I am writing to express my grave concerns regarding the Cybercrime Bill currently under consideration by the Joint Select Committee. As chairman of the Law Reform Commission, I understand that your aim is to enact legislation that addresses the growing challenges posed by online misconduct while safeguarding individuals' rights to free speech. However, upon reviewing the provisions of the bill, I am deeply troubled by its potential implications for freedom of expression, particularly in the context of political discourse.

The provision that penalizes individuals for disseminating content that may cause emotional distress, regardless of its veracity, raises serious concerns about the stifling of dissent and criticism, particularly in the realm of political commentary.

In a democratic society, the ability to engage in robust debate and express diverse viewpoints is fundamental to holding our elected representatives accountable. However, the ambiguous language of the bill could inadvertently silence individuals who seek to comment on political issues, especially those that may provoke emotional reactions from members of parliament.

Moreover, the formation of a Joint Select Committee to review the bill has been criticized as contrary to parliamentary procedure, further undermining public trust in the legislative process. As chairman of the Law Reform Commission, I urge you to reconsider the relevant and offending provisions of the Cybercrime Bill to ensure that they do not infringe upon individuals' rights to free speech and political expression.

Furthermore, I seek clarification on how bloggers can continue to operate within the confines of the law if the information they present, whether true or untrue, has the potential to cause emotional distress to others. Given the broad scope of the bill's provisions, it is essential that bloggers receive clear guidance on navigating the legal landscape to avoid inadvertently violating its provisions.

In conclusion, I implore you to address these concerns and ensure that the Cybercrime Bill strikes an appropriate balance between combating online misconduct and upholding fundamental rights to free speech and political expression. Failure to do so risks undermining the very principles of democracy and transparency that form the foundation of our society.

Thank you for your attention to this matter.

Regards
Peter MacD Earle BSc, LLM

Peter Earle <peterearlebb@yahoo.co.uk> 4/25/2024 10:00 AM

Response to the Chairman's remarks targeting critics of the Cybercrime Bill

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Sir David Simmons

Chairman,

Law Reform Commission

Dear Sir David Simmons,

Re: Response to Nation News Article of Tuesday April 23, 2024

Your defense of the Cybercrime Bill as articulated in the Nation newspaper of Tuesday 23 April 2024, raises several points that warrant scrutiny and critique.

Firstly, while you emphasized that Barbadians are free to transmit data as long as it does not defame others or cause distress, the bill's language regarding causing emotional distress is vague and subjective. This ambiguity opens the door to potential abuse, as individuals may be hesitant to engage in legitimate criticism or political discourse out of fear of inadvertently causing distress to others.

Furthermore, the examples provided of computer misuse, such as the reception of pornographic content or false allegations, do not warrant the extensive scope of the proposed bill. While it is crucial to tackle such abuses, this should not be done at the cost of suppressing free speech or deterring lawful expression. It is noteworthy that no instances were cited where individuals might levy baseless accusations.

Your assertion that the bill contains defenses for truth, comment, triviality, and privilege is not sufficient to allay concerns about its potential impact on free speech. The burden should not solely rest on individuals to defend themselves against allegations of causing distress, especially when the interpretation of such terms is left to the courts.

Additionally, Sir David, your dismissal of criticisms from individuals like Caswell Franklyn and others as not drawing attention to the bill's provisions for defense overlooks the broader concerns about the bill's potential chilling effect on speech. Rather than dismissing critics, it would be more constructive to engage with their concerns and address them transparently. I hope that at some time, since you singled them out that you meet with these Individuals to discuss their concerns.

As the bill moves forward, it is essential to strike a balance between protecting individuals from harm and upholding fundamental rights to free speech and political expression. Therefore, I urge you and the Law Reform Commission to reconsider the relevant provisions of the bill and ensure that it does not unduly restrict public discourse and criticism.

Many bloggers at the moment are afraid that the bill will not allow them to continue blogging under the bill's provisions. In this regard I am seeking clarification from you and the Law Reform Commission on how the bill will impact online commentary and what safeguards are in place to protect freedom of expression. It is crucial for bloggers and online commentators to understand their rights and responsibilities under the law to avoid unintended legal consequences.

Specifically, I am interested in knowing if, based on the provisions of the bill and considering that the Marcia Weekes Show has disseminated public information on issues like the HOPE Project, Marcia Weekes, Kemar Stuart, and Caswell Franklyn would face the risk of incurring a $70,000 fine or a 7-year prison sentence if any individual associated with the HOPE project, whose name was mentioned, became emotionally distressed.

In conclusion, while your defense of the Cybercrime Bill highlights the need to address online misconduct, it fails to adequately address the legitimate concerns about its potential impact on freedom of expression.

I eagerly await a response from you and the Commission.

Regards
Peter MacD Earle BSc, LLM

Grenville Phillips <nextparty246@gmail.com> 4/25/2024 10:47 AM

Solutions Barbados' Comments on the Cybercrime Bill

To Parliament of Barbados <parliamentbarbados@caribsurf.com>

Dear Clerk of Parliament:

1. Solutions Barbados hereby responds to the Joint Select Committee's public invitation to share our concerns with the Cybercrime Bill (2024).

2. Our comments are attached. Please confirm receipt of the four-page correspondence.

3. We hereby confirm our willingness to appear before the Committee to make an oral presentation and respond to any queries the Committee may have.

Best regards,
SOLUTIONS BARBADOS

Grenville Phillips II
President
Cell/WhatsApp: (246) 232-9783

- Solutions Barbados - Joint Select Committee - Cybercrime Bill.pdf (524 KB)

SOLUTIONS BARBADOS
The Way Forward

Solving Problems that are Hindering Barbados' Development.

Cell/WhatsApp: (246) 232-9783 • E-mail: NextParty246@gmail.com • Web: SolutionsBarbados.com

25th April 2024

Parliament of Barbados
Parliament Buildings
Trafalgar Street
BARBADOS

Attention: Clerk of Parliament

Re: Cybercrime Bill

Dear Sir:

Solutions Barbados hereby responds to the Joint Select Committee's public invitation to share our concerns with the Cybercrime Bill (2024). Our concerns follow.

1. Lowering the Threshold of Guilt to Punish the Innocent

The Cybercrime Bill is intended to repeal the Computer Misuse Act (2007). Both documents are similar. However, the Cybercrime Bill makes it much easier to: (i) make innocent persons guilty of new crimes and (ii) punish them severely.

Our main concern with the Cybercrime bill is Section 20 (1) which states.

> *"A person who intentionally uses a computer system*
>
> *(a) to publish, broadcast or transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene or of a menacing character or causes any such data to be so sent;*
>
> *(b) for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress to that person, is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both."*

The offensive parts of Section 20 (1) follow.

> *"A person who intentionally uses a computer system to publish ... data that is offensive ... for the purpose of causing annoyance ... [or] embarrassment ... is*

guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both."

The corresponding section in the Computer Misuse Act (Section 14) states.

Where a person uses a computer to send a message, letter, electronic communication or article of any description that

(a) is indecent or obscene;

(b) is or constitutes a threat; or

(c) is menacing in character,

and he intends to cause or is reckless as to whether he causes annoyance, inconvenience, distress or anxiety to the recipient or to any other person to whom he intends it or its contents to be communicated, he is guilty of an offence and is liable on summary conviction to a fine of $10 000 or to imprisonment for a term of 12 months or to both."

In the Computer Misuse Act, the hurdles to be cleared to be found guilty are:

1. use a computer to send a message, letter, electronic mail or article;
2. the message had to be indecent, obscene, threatening, or menacing; and
3. the messenger intended to cause or was reckless as to whether he caused annoyance, inconvenience, distress or anxiety to the recipient.

In the Cybercrime Bill, any offensive data that is published for the purpose of causing annoyance or embarrassment is a new crime. This data is not limited to being a message, letter, e-mail or article as in the Computer Misuse Act to guide the judge. Instead, it is defined as *"data that is offensive"*. This could include statistical information like inflation, unemployment or debt that may offend, embarrass or annoy the politicians who were managing the economy during the time range of the reported statistics.

Who determines what is offensive? The Computer Misuse Act defines the scope of what is offensive to guide the judge, namely: indecent, obscene, threatening or menacing. The Cybercrime Bill gives no such scope or guidance but gives the judge wide discretion. This uncertainty can only be risky for accused persons. Clearly, high unemployment rates and unsustainable national debt figures are embarrassing to government Ministers – and they should be, so that they may be motivated to do better.

Is it reasonable for politicians to be: (i) embarrassed by the publication of unfavourable statistics and (ii) annoyed by the repeated publication of statistics that could support accusations of their incompetence? Of course. However, under the Cybercrime Bill, the

persons who post such unfavourable data on their social media accounts have likely posted evidence that proves their guilt, making them liable *"to a fine of $70 000 or to imprisonment for a term of 7 years or to both."*

2. Bill of Political Intimidation

The change in language from the Computer Misuse Act (Section 14) to the Cybercrime Bill (Section 20 (1)), suggests that the new intent of the Cybercrime Bill may be to stop Barbadians from commenting publicly on social media where such comments may embarrass the Government. It seems crafted to misuse a Bill originally intended to punish actual cybercrimes (like cyber terrorism and child pornography) and use it to intimidate Barbadians into silence through fear. Therefore, the Bill appears to be in violation of its own Section 19.(1), which reads.

> *"A person who intentionally or recklessly uses a computer system to publish, broadcast or transmit computer data that intimidates a person ... is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both."*

3. Shifting Blame

When we complained about the highly offensive nature of Section 20.(1), we were informed that our Bill was not a homegrown initiative but was modelled from a Council of Europe treaty agreed in Budapest in 2001 called *"Convention on Cybercrime"*. If this is true, then the former European enslavers seem determined to enslave us by making us all guilty, and then maintaining their control by keeping us in perpetual fear. To investigate the truth, we read the Convention.

The European convention does not contain any of these ridiculous offenses and unconscionable punishments specified in our Cybercrime Bill. Instead, Article 13 of the Convention requires each Party to adopt proportionate sanctions. How is $70,000 and/or 7 years imprisonment for causing someone *"annoyance"* even remotely proportionate? Who increased the penalties from $10 000 and/or 1 year imprisonment in the Computer Misuse Act? It seems that we want to harm each other and blame others for our cruelty.

4. Violating Civil and Political Rights

Article 15 of the Convention requires each Party to provide safeguards that *"shall provide for the adequate protection of human rights and liberties ... , including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966*

United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality."

Article 14, Section 3 (g) of the International Covenant on Civil and Political Rights states.

> *"In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality: Not to be compelled to testify against himself or to confess guilt."* (Bold emphasis ours)

In the Cybercrime Bill (Section 24. (1) and (2)), if you do not help the police obtain evidence to convict you, including providing passwords and decryption information, then you are guilty of an offence. If you ask your employee not to help the police, then you are also guilty of an offence and are liable *"to a fine of $25 000 or to imprisonment for a term of 2 years or to both."*

5. Conclusions and Recommendations

The original purpose of the Cybercrime Bill, which was to punish those guilty of actual cybercrimes, was good. The homegrown additions to intimidate Barbadians into silence on social media by inventing new cybercrimes, is very bad. In the Cybercrime Bill, the bad far outweighs the originally intended good to the point that if the Bill is proclaimed in its current form, it will be a foreseen danger to the public.

Since the Cybercrime Bill must be passed, we recommend the following critical amendments.

1. Replace Section 20 (1) with Section 14 of the Computer Misuse Act.
2. Omit Section 24. (1) and (2) which appears to be a violation of civil and political rights.

Since other bills will likely be passed that may avoid scrutiny, it is important that we use this opportunity to mitigate foreseen danger, by asking those who drafted this bill to justify why they inserted the highly offensive sections.

Yours respectfully,
Solutions Barbados

Grenville Phillips II
President

Yokaana Moore <yokaanamoore@gmail.com> 4/25/2024 12:12 PM

The Cybercrime Bill, 2024

To parliamentbarbados@caribsurf.com

Petition Against the Cybercrime Bill, 2024

To The Honourable Members of the Barbados Parliament:

We, the citizens of Barbados, strongly object to the proposed Cybercrime Bill, 2024, and demand its immediate withdrawal. While recognizing the importance of addressing cyber threats and ensuring digital security, we believe that certain provisions in the bill have far-reaching implications for individual rights, privacy, and civil liberties.

The bill threatens to violate our rights to privacy, freedom of expression, and access to information online. It may give the government unprecedented power to monitor and control our online activities, potentially leading to censorship and surveillance of innocent citizens.

Reasons for Our Opposition:

Threat to Freedom of Expression: The bill's vague and broad language criminalizes legitimate online activities, including criticism of the government and peaceful dissent. It will stifle public discourse and undermine our fundamental right to express our views freely.

Overreach of Police Powers: The bill lacks adequate safeguards for data privacy. It gives police sweeping powers to intercept electronic communications, search and seize electronic devices, and detain individuals without proper safeguards. This excessive authority poses a serious threat to privacy and due process.

Cybersecurity Threats: While the government claims the bill will enhance cybersecurity, experts have cautioned that it will weaken our defenses by creating vulnerabilities and promoting distrust among the public.

Economic Impact: The bill imposes severe penalties, including a lengthy imprisonment term, and this terrifying effect on online activities will discourage investment, innovation, and job creation in the technology sector.

International Reputation: The passage of this bill will damage Barbados' international reputation as a democracy that respects human rights and fundamental freedoms.

We therefore demand that the government withdraw the Cybercrime Bill immediately and engage in a transparent and inclusive public consultation process to develop a comprehensive and balanced cybercrime law that protects both public safety and civil liberties, and to ensure that any future cybercrime legislation complies with international human rights standards, while safeguarding the privacy and free speech rights of Barbadians.

Yokaana Moore
yokaanamoore@gmail.com

Jeanie Mottley <jeaniemottley@gmail.com> 4/25/2024 1:25 PM

Submission regarding the Cyber Crime Bill

To parliamentbarbados@caribsurf.com

Good afternoon,

Please accept my comments regarding the Cybercrime Bill which is currently being reviewed.

Have a wonderful day!

Best Regards

Jeanie Mottley (Mrs.)

- Parliament - Cybercrime Submission.docx (29 KB)

To: Joint Select Committee:

From: Mrs. Jeanie Mottley

Date: Thursday April 25th, 2024

Subject: Cybercrime Bill: Important concern re *Cyber Bullying Section 20.* ***(1)***

The cybercrime bill in its current form with respect to **sections 20. (1) Cyber bullying** will criminalize a person or group of persons. This section has troublesome language, which is vague and will be hard for a person or group of persons to prove their innocence if the bill is proclaimed in its present form. The Bill unintentionally gives power to the Magistrate to interpret what the bill intends which is not fair, equitable and transparent since as human beings we all have our inherent biases.

Cyber bullying

A person who intentionally uses a computer system to publish, broadcast or transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene or of a menacing character or causes any such data to be so sent; for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress"

Example One

Our National newspapers who have online publications can run afoul of this section of the bill. They publish court appearances including persons faces, addresses and what they have been charged for (The person at this time is still innocent until proven guilty) Such publications cause humiliation, anxiety, and substantial emotional distress to the person whose matters are being published. Their hurt and embarrassment is etched in print and on computers for time immemorial.

What are the criteria for judging that the online newspaper's publishing of the person's most embarrassing moment in life was not done for the purpose of humiliating the accused and profiting at their expense? , (Did the reporter not deliberately go to the court to get the story?) and surely they know that publishing this information about the accused can cause others to express hatred, insult and even intimidation towards the accused.

When that person has been found not guilty can the humiliation, anxiety, and substantial emotional distress he or she suffered be undone? Under this Bill I find that the Reporter and Editor of our National online newspapers may be found guilty.

Example Two

Our online social media platforms can be criminalized under Cyber bullying. Case in point, the situation whereby a thief stole a cheque from a Constituency Office. This was factual according to the Police, our national newspapers and according to the Minister in question.

Social media platforms discussed this matter and the discussion spilled over onto radio programs and voice notes were sent among the population questioning whose name was on the cheque and the legality of it and whether there was perceived appearance of impropriety. There is no doubt that this caused humiliation and substantial emotional distress towards the Minister in question.

What are the criteria to determine whether the Social Media platform broadcast of the theft of the cheque and the Minister's involvement was for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress?

Social Media platforms could argue that they shared and discussed news that was already in the public domain and confirmed to be correct by our trusted newspapers and Police force. They even took the Minister's word that the cheque was in their name.

If the Minister says he/she was humiliated and is experiencing substantial emotional distress, then Under this Bill I find the Social Media Platforms may be found guilty.

Example Three

A Nigerian woman who wrote an online review of a can of Tomato puree is facing imprisonment in her country after its manufacturer accused her of "malicious allegations" In her review she said to her audience "Help me advise your brother to stop killing people with this product, yesterday was my first time of using and its pure sugar." Under this Bill she could be found guilty.

In closing I suggest that there should be a glossary attached to this Bill which clearly and succinctly explains the terms used to define cyberbullying. Consideration should be given to each of the Words outlined under the Cybercrime Heading. For example.

Intent to cause:

Substantive Humiliation:

1. If the matter reported is factual but the public has a right to know since the person is a public official, is it a crime if as a result the public official experienced humiliation?
2. If the person is an unknown citizen and the matter reported is factual and the newspaper publishes the story on its online platform to increase readership and financial gains. Is it a crime because the unknown citizen is humiliated?
3. Substantive Humiliation is different for everyone. What examples of humiliation are defined under this bill?
4. Can the damage to the person as a result of Substantive Humiliation be measured. What are the measures which constitute a crime under this bill?

I thank you for your consideration of the points I have made and hope that we can amend this Bill so that it only prosecutes true criminal intent and avoids unjust prosecutions.

J Lloyd <jl1190133@gmail.com> 4/25/2024 2:07 PM

My comments on the Cybercrime Bill of 2024

To parliamentbarbados@caribsurf.com

Dear Sir/Madam,

I submit the following comments regarding the Cybercrime Bill.

My name is John Lloyd, I am a temporary resident of Barbados and have had a lifelong interest in cyber security and cyber defences for ordinary people.

The following comments reflect my knowledge of legal issues and industry concerns regarding this topic.

best regards

John Lloyd

Comments follow:

re Cybercrime Bill 2024 currently at the Senate of Barbados:

This bill has some important issues for the following types of people and activities:

1. Research into cyber crime, including means and ways to discover defects in a "computer system" that may permit or enable access that is otherwise unauthorized.

See para 11(1).

It is an important part of worldwide cyber defence activities to allow, and encourage, testing and discovery of defects that are exploitable. In normal course, a cyber security researcher works on an isolated copy of a computer system, but also may access public services, e.g. Google search, or systems publicly visible such as a wifi router, or systems accessible through a publicly visible connection such as a webmail portal.

The law should explicitly allow for non-destructive research discoveries, which combined with disclosure to the owner of a "computer system" or the manufacturer of a "computer system" that defects exist and ought to be remediated. It should be listed as a defence that both authorized intrusion testing and non-destructive unauthorized testing for the purposes of cyber safety should be allowed. Some additional definitions may be needed.

It is also a world-wide general policy on the part of most security researchers to provide as little as 90 days notice to the system owner or manufacturer of a publicly visible security defect before publication. The motive is to create urgency for repair of defects. There are dozens of such disclosures worldwide every week. The laws of Barbados ought not to categorize such disclosures as criminal unless some evidence of malicious intent is met.

There are numerous cases worldwide, e.g. UK, US, Turkey, where well-meaning good Samaritans have privately disclosed exploitable defects to the operators of publicly accessible systems (web sites, transit

systems, etc) only to be prosecuted for a cyber crime without any evidence of malicious intent by the Samaritan.

2. The law provides a "likelihood" test (Para 19(3)) for injury due to contempt, embarrassment or ridicule. This is too low a barrier. The publication of political cartoons is often intended, and likely, to mock or embarrass politicians. The Defamation Act would appear to provide a defence however it is the risk of unnecessary prosecution that should be addressed here. "Likelihood" should be replaced with "proven" injury.

Compare para 20(1) where "causation" is a necessary element of the offence.

3. The definition of "service provider" (para 2(1)) includes "any entity" which would seem to include any person in possession of a computer that processes data on their own behalf. Combined with the enforcement and evidence provisions of para 23 and subsequent, it seems any resident of Barbados would be subject to orders requiring decryption of personal data, disclosure of personal financial, personal or social data.

The mandatory decryption of sensitive data seems to be a new authority and is not evidently part of the public discussion surrounding this proposed law.

4. The confidentiality requirement (para 28(2)(c)) regarding the existance or content of a preservation order seems to preclude countervailing actions brought to court to overturn or modify such an order. A person must have the right of due process to challenge an order, even an ex parte order. This paragraph seems to overturn due process rights.

jazzmal2023@outlook.com <jazzmal2023@outlook.com> 4/25/2024 2:52 PM

Cyber Crime bill

To parliamentbarbados@Caribsurf.com <parliamentbarbados@caribsurf.com>

This mail has no content

- Cybercrime bill.docx (18 KB)

Re: Cybercrime Bill.

There are many relevant and acceptable areas of the bill. However, there are other areas which I find concerning.

These are the sections of most concern:

1 Under the Malicious Communication heading, Sections 19.3 and19.5.

2. Under the Search and Seizure heading. Section 23.

3. Under the Assisting a Police Officer heading, Section 24.

In some of these sections, the language is not precise enough. The vague nature of the language lends itself to too much subjectivity in its interpretation Clarity is needed.

Sheldon Mottley <sheldonomottley@gmail.com> 4/25/2024 3:25 PM

Cybercrime Bill matters and concerns April 2024

To parliamentbarbados@caribsurf.com

To: The Clarke of Parliament
Re: The Cybercrime Bill

I hereby submit my objections to the honorable members of the Joint Select Committe reference the Cybercrime Bill in its current form.

The Constitution of Barbados is the supreme law of this territory and jurisdiction. Any Bill in conflict with the Constitution, whether in whole or in part, is null and void to the extent that it conflicts against the Constitution of Barbados.

In addition, The Universal Declaration of Human Rights of the United Nations, of which Barbados is an active member and signatory guarantees each man, woman and child in Barbados the following:

Freedom of Speech
Freedom of expression and opinion
Freedom of movement
Freedom of peaceful assembly and association
Article 18 Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his/her religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.

Article 19 Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Sir, I refer the Joint Select Committee on the Cybercrime Bill to Articles 1 to 30 of The Universal Declaration of Human Rights which is enshrined by the United Nations.

I therefore stand on the Constitution of Barbados and the UDHR and state that the Cybercrime Bill in its current form will infringe on the freedoms and rights of Barbadians now and for generations to come. It cannot be passed into law in Barbados.

The language of the Cybercrime Bill is too wide, vague and ill defined.
The Bill whether intentional or unintentionally will stifle and muzzle the freedom of expression and opinion and movement and free association of Barbadians.
The Bill will prohibit and muzzle all constructive criticism of the government, as well as alternative proposals and options to to what the government may propose to do in Barbados whether or not barbadians are in favor of what may be planned.
One may be forced to give access to the police to personal devices storing intellectual and copy right materials, medical and legal information, investment and financial information, business competitive data, private family information etcetera which cannot be divulged and which has nothing to do with the allegations being charged against you and your alleged misuse of data.
The penalties are draconian, invasive and disproportionate.

I cannot support the Cybercrime Bill in its current form nor will I .
In addition, The Mutual Assistance in Criminal Matters Act, Cap 140A would in essence be giving the Cybercrime Bill in its current form, iron teeth.

Thank you for considering this submission in the good practice of democracy.

Sheldon Mottley
A concerned national of Barbados

Rosaline Corbin <rjcbarak@yahoo.com> 4/26/2024 7:42 AM

Submission re The Cybercrime Bill

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Attention: The Clerk of Parliament

Please find attached my submission re The Cybercrime Bill.

Thank you.

Rosaline J. Corbin (Mrs.)
JP, Postgrad Dip.Ed., M.Ed. (Manchester University, UK)

Rosaline

- Submission To Joint Select Committee Cybercrime bill - In Whose Interest.docx (21 KB)

The Cybercrime Bill, 2024 ...In Whose Interest?

Term of Reference, Number 1 for the Joint Select Committee (Standing) On Governance And Policy Matters On The Cybercrime Bill, 2024 And Mutual Assistance In Criminal Matters (Amendment) Bill is given as...

To enquire into and determine whether the Cybercrime Bill as drafted fulfils the expressed purposes to ensure compliance with the International Conventions, global standards and best practices to counter cybercrime and to ensure international cooperation in the combatting of cybercrime.

As stated in this term of reference, it can be seen, from the outset, that the drafted Cybercrime Bill seeks to satisfy the requirements and interest of external entities. The intent could be implied as, "Make sure we have dotted the i's and crossed the t's to meet the approval and acceptance of the International Conventions, namely The Convention on Cybercrime also known as the Budapest Convention.

According to the online Collins Dictionary: "If you refer to an express intention or purpose, you are emphasizing that is a deliberate and specific one that you have before you do something".

Would our thinking and questioning be flawed if we were to surmise that the reason, aim or objective behind this Bill is driven by the demands of these conventions to which we have signed on, and the haste to respond? Are we saying: satisfy and please the global sphere, then let's attend to domestic/national matters, framing our own legislation in a way so as not to compromise what we have signed on to? In whose interest is this Cybercrime Bill? This Bill borrows from the legislative framework of The Convention on Cybercrime also known as the Budapest Convention, and was facilitated in its drafting by consultants from the Council of Europe. Obviously it is to satisfy their interests.

This submission draws also from statements by the Honourable Marsha Caddle, M.P. in her capacity as Minister of Industry, Innovation, Science and Technology who led off the debate on February 4, 2024 on the Cybercrime Bill. She expressed that through this Bill, Barbados would have in place the legislative framework to meet international requirements and enable international cooperation as it relates to cybercrime across jurisdictions. Minister Caddle also noted that much of the cybercrime does not originate domestically but rather across international borders, and spoke of the reach of this bill to Barbadians outside of Barbados who may be suspected and charged of cybercrime.

It would be remiss of this author to be dismissive of any attempt to protect our country and people from cybercrime, including cyber terrorism, computer related fraud and computer related forgery at the personal as well as national level. Safeguards are needed and yes, facilitated through legislation, but not at the risk of instituting and legalising measures which can be construed as intimidating and restrictive, for example, Part II of the Bill captioned PROHIBITED CONDUCT, Section 19 Malicious Communications, as well as Part III captioned INVESTIGATION AND ENFORCEMENT almost in its entirety.

The author of this submission supports wholeheartedly and emphatically the Sections 16,17 and 18 respectively relating to Child Pornography, Child Grooming, and Online Child Sexual Abuse.

One would hope that this Cybercrime Bill is not the boastful outcome of an exercise in proving that Barbados is ahead of the game, to be held up as an exemplar as a small island developing state in being responsive to the International Conventions.

It would seem that the number 1 Term of Reference has already met the requirement of the International Conventions given the comments attributed in the press to the Attorney General who remarked that the consultants from the Council of Europe said "Barbados now has the finest legislation on cybercrime anywhere in the region". Is Term of Reference Number 1 redundant?

Now it leaves us to be as copious and diligent in attending to the other Terms of Reference under scrutiny before this Joint Select Committee, ensuring that all persons are treated fairly under the law(s) of this land.

Thank you.

Submitted by:

Rosaline J. Corbin (Mrs.)

JP, Postgrad Dip.Ed., M.Ed. (Manchester University, UK)

Rosaline Corbin <rjcbarak@yahoo.com> 4/26/2024 11:25 AM

Submission - Specific Groups

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Attention: The Clerk of Parliament

Thank you for acknowledging my previous submission.

Please find attached a second submission from me re The Cybercrime Bill.

I wish to also make an oral presentation before the Joint Select Committee for the Cybercrime Bill.

Thank you.

Rosaline J. Corbin (Mrs.)
JP, Postgrad Dip.Ed., M.Ed. (Manchester University, UK)

Rosaline

- Submission Specific Groups.docx (23 KB)

SUBJECT: Specific Categories of Persons

This submission speaks to Term of Reference. Number 4, which reads:

To examine whether the Cybercrime Bill as drafted provides adequate protection to all of the specific categories of persons who may potentially be vulnerable to cybercrime.

Who are these specific categories of persons? These should be identified and not left to assumptions and subjectivity. What is meant by "adequate protection" and by whom?

One does not see provision for adequate protection in the Bill beyond "the protection of legitimate interests in the use and development of information technologies" as stated under caption OBJECTS AND REASONS (b).

Recalling the speech of the Honourable Marsha Caddle, M.P. in her capacity as Minister of Industry, Innovation, Science and Technology who led off the debate on February 4, 2024 on the Cybercrime Bill, one heard general reference to persons who are vulnerable, but no specific category of these persons was identified beyond minors and IT "experts". Of the latter, the Minister said they would not be criminalised and penalised if their work requires them to engage in lawful legitimate hacking and can be deemed as so.

The author of this submission would like to draw to the attention of this Joint Select Committee, in her opinion, the category of persons who could be described as **maybe potentially vulnerable to cybercrime** and who need to be assured that the Cybercrime Bill provides adequate protection for them.

Who are these groups of persons? This presenter sees them as seniors, the differently abled, and the minor, who unknowingly could be exposed through another who perpetuates the crime using the devices of these persons.

Scenario: The senior person has a cell phone or laptop. The device needs repair work. The senior takes it to a technician to troubleshoot or repair. The technician, unknowing to the senior, uses the opportunity to engage in some form of cybercrime or any of the actions classified as prohibited conduct, e.g. malicious communication, child pornography. Law enforcement officers turn up at the senior's door with a warrant to search, and seize the device and arrest. Senior is traumatized and shocked because senior does not know why or for what he or she is being charged. Senior protests vehemently and pleads innocence, which is really so. Is the Senior

considered a victim or perpetrator of the crime, and if a victim, how will this be proved, how long will it take to be solved, where will the Senior, a pensioner in most cases, have the funds to retain legal representation before the courts, and hanging over his or her head - a penalty of $70,000 Bds or 7 years in jail.

This author is aware of seniors who are already becoming suspicious of persons wanting to use their cell phones or other devices, giving the possible inappropriate use of their cell phone or device by another and how they can be implicated. Trust is being undermined and suspicion is being heightened.

The above scenario can be played out with a senior or any other person in a household or other settings where someone takes up another person's phone or device, and uses it deliberately or maliciously to defraud or bully another person. How is the owner of the device protected under this Cybercrime Bill?

Now on to the minors.

Children today seem to be born with an electronic device in their hand and embedded with an IT DNA. We know that they use their devices to create, capture, and transmit information and images which can be deemed as criminal actions under this Cybercrime Bill; malicious communication, pornography, cyberbullying. The quickest thing our youth can do is to whip out their cellphones and they do not discriminate, neither are they selective in what they post and what they forward. How will these minors be treated under the law as presented in the Cybercrime Bill? Are these minors made aware of how this Cybercrime Bill can affect them now and in their future?

In the debate which was cited earlier, the Minister (Caddle) spoke of the consultations, engagements and workshops which occurred in the preparation of the draft Bill. Mention was made of speaking with experts globally, regionally and nationally; that workshops were conducted with the judicial as well as police officers – the main players in monitoring and enforcing the law under the Cybercrime Bill. In addition, she shared that sessions were held with the service providers in the private sector who offer international services and who can be considered to be more prone and susceptible to cybercrime.

This author perceives the process engaged to produce the Cybercrime Bill to be the usual top-down approach, and the proverbial ordinary citizen has been left wondering and questioning how will this Cybercrime Bill affect them, and are concerned about their freedom of expression, and most disconcertingly, treatment at the hands of the police, possible charge and arrest, fines and alternative

imprisonment. The Minister says that she believes in, and practices, the conversational approach and welcomes ongoing conversation as it relates to this Cybercrime Bill. Will this happen and how soon, beyond these submissions, which only a few interested persons are participating in? In fact, many persons are unaware of the existence of this Joint Select Committee and that written submissions can be sent as well as oral presentations made before the Committee.

Minister Caddle quoted that in 2022, there were 235,000 internet users and 328,00 mobile connections in Barbados. Amongst these are those specific categories of persons spoken of in this submission, namely the seniors, minors, and differently able, who in the presenter's opinion are not provided within the Cybercrime Bill and who will be affected.

This submission asks that Term of Reference 4 be examined to:

Identify and widen the scope of the specific categories of persons, giving examples where possible, of who may potentially be vulnerable to cybercrime other than those listed already in the Bill.

Explain / state what constitutes "adequate protection" for these persons.

Thank you.

Submitted by:

Rosaline J. Corbin (Mrs.)

JP, Postgrad Dip.Ed., M.Ed. (Manchester University, UK)

Dave & Marcia <dm_weekes@yahoo.com> 4/26/2024 8:47 AM

Citizen's comments in regard to the Cybercrimes Bill

To Parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com> Copy
Kathy Weekes <kathann_kw@yahoo.com> • Sean & Lee (Apache) Carter <apacheintl@gmail.com> •
Lisa Niles <lmichelleniles@gmail.com>

Dear Sir/Madam,

Please find attached my feelings and beliefs with regard to some of the content of the recent Cybercrimes Bill. I would be grateful if these comments are considered in the process of re-drafting the bill.

Thank You,
Dave & Marcia Weekes (Praise Academy & Step By Step Productions)
246-439-7000 (Office)
246-236-7000 (Cell)
516-345-8066 (Magic Jack)
www.praiseacademyofdance.org
Rent or Download our movies @

JOSEPH www.vimeo.com/ondemand/joseph2

Barrow - Freedom Fighter
www.amazon.com/Barrow-Freedom-Fighter-Adrian-Holmes/dp/B088P8TH5D

Vigilante - The Crossing
www.amazon.com/Vigilante-Crossing-Malissa-Alanna/dp/B081KXMJLS

Chrissy www.vimeo.com/ondemand/chrissy

HUSH 2 www.vimeo.com/ondemand/hush2endthesilence

HUSH 3
www.vimeo.com/ondemand/hush3twistedinnocence

HUSH 1 www.vimeo.com/ondemand/hush1

- Concerns About The Cybercrimes Bill.pdf (129 KB)

My Concerns About The Present Content of the Cybercrimes Bill

I believe that in this new world where the computer and other devises permit invisible communicate to and from anywhere in the world, that our government needs to protect its citizens from crimes which we have seen perpetrated online.

We are in favour of having a Cybercrimes Bill. We commend our government on the initiative to have such a Bill. However, as thinking, voting citizens, in reading the Bill there are some clauses which we believe are detrimental to the freedoms we have enjoyed over the years. We wish these section or clauses removed from the bill. These are:

In Section 19(1)(a) the Bill speaks to "Intimidation" as grounds for cyber protection. The truth is that intimidation is an emotional state of mind and occurs daily under normal circumstances in life. Boxers are intimidated by bigger, stronger more experienced boxers, Teachers can be intimidated by a seasoned no-nonsense Principal and the list goes one. In neither of these circumstances is the intimidating Boxer or Principal expected to appear before the law courts and face criminal charges. The law courts themselves are intimidatory in nature. Hence the grounds of "intimidation" as a single pilar of offense needs to be removed from the Bill as a potential for cybercrime.

In Section 19(3) the Bill refers to "ridicule", "contempt" and "embarrassment" as grounds for an offence in cyberworld. I believe again that this is unreasonable, notwithstanding, the extreme punishment of a $70,000 fine or 7 years imprisonment, if found guilty. Ridicule, contempt and embarrassment among other social emotions are facets of normal life and many times, helps us to mature. To use these subjective facets as measures of criminal deviance is extreme and also need to struck from the Bill.

While the Bill may wish to deal with what it terms "malicious communication" and rightfully so, extreme caution, consultation and due diligence must be completed in order to ensure the rights and freedoms of citizens are no compromised. I believe, in this context, where the term "malicious" is by nature subjective, that maybe a series of warnings, non-intrusive monitoring and test for consistency of mal-doing be enforced such that the Bill recognizes and is able to establish mal-intent on the part of the perpetrator before criminal charges are brought.

We thank you for this opportunity as a voting citizen of Barbados.

Dave Weekes

m.bayley17@icloud.com 4/26/2024 9:23 AM

To the Clerk of Parliament - Cybercrime Bill, 2024 submission

To parliamentbarbados@caribsurf.com

Good morning Sir,
Please accept the attached document as my submission setting out my views and comments on aspects of the bill.

I do not want to appear in person before the Committee.

Warm regards,
Michelle Bayley, CPA, CGA, FCA

- Submission re Cyber Crime bill.pdf (740 KB)

A REVIEW OF SECTION 23(2)

DATA DAMAGE AND LIABILITY IN THE BARBADOS CYBERCRIME BILL

SUBMITTED BY MICHELLE BAYLEY

Proposed Amendments to Section 23(2) of the Barbados Cybercrime Act".

Cybercrime in the digital age has emerged as a significant threat to individuals and nations. Many countries, including Barbados, have enacted comprehensive cybercrime laws to combat this. The Barbados Cybercrime Bill 2024 is designed to deter and punish cybercriminals. However, like any legislation, this kind requires continuous review and amendment to remain effective and just. This article focuses on Section 23 Subsection (2) of the Act, which grants police officers broad powers during cybercrime investigations. While this provision is crucial for law enforcement, it raises concerns about the technical expertise required to execute its mandates effectively and the potential for mishandling ***personal data in evidence gathering where officers are given broad authorization during investigations involving computer systems and data.*** Herein, we review these issues and propose amendments to enhance the Cybercrime Bill's effectiveness while ensuring the integrity of digital evidence.

Flawed Aspects of Section (2):

- **Lack of Specificity for Technical Tasks:** The section empowers police officers to perform actions like using decryption technologies (paragraph (d)) and maintaining data integrity (paragraph (g)). These tasks necessitate specialized knowledge in cryptography, data management, and computer forensics, which basic police training may not adequately cover.

- **Potential for Evidence Compromise:** Improper handling of digital evidence during data seizure, analysis, or storage can lead to its exclusion from court. The **UK Guardian**[1] newspaper, in the 2018 article titled – "***Police mishandling digital evidence, forensic experts warn,***" retrieved from https://www.theguardian.com/law/2018/may/15/police-mishandling-digital-evidence-forensic-experts-warn, states the following:

> "Giving evidence to a justice select committee inquiry into failures to hand over material that have led to multiple court cases collapsing, leading digital forensic experts warned of funding shortfalls and inadequate skills."

[1] https://www.theguardian.com/law/2018/may/15/police-mishandling-digital-evidence-forensic-experts-warn

The writer further noted that:

> "Police officers are trampling over vital forensic evidence, are under-trained, and often do not know what they are looking for, MPs investigating digital disclosure problems have been told.
>
> Giving evidence to a justice select committee inquiry into failures to hand over material that have led to multiple court cases collapsing, leading digital forensic experts warned of funding shortfalls and inadequate skills. .... When I first started, the police had their own digital forensic units and knew 'what they were about.' Now, you are getting very sketchy evidence. People give me screenshots of pictures of a phone. I need to see [a copy of the] original, be able to repeat and verify tests."

- **Silence on Liability Remedy for Data Damage or Accidental Erasure**

  Given the broad investigative power accorded by law enforcement, including data seizure, the section is silent on liability and the remedy afforded to the accused if said person's data is damaged in any way during the retrieval process by law enforcement. This is a possibility, and if the damage is unrepairable, the bill should provide recourse to compensatory damages for the affected person.

Proposed Amendments:

Current wording of Subsection (2)(d):

(d) have access to any information, code, or technology which has the capability of transforming or converting an encrypted program or data held in or available to the computer system into readable and comprehensible format or text, for the purpose of investigating any offence.

Proposed Amendment 1: Inclusion of Experts

New wording:

(d) in consultation with a qualified cryptologist or computer forensic expert, have access to any information code or technology which has the capability of transforming or converting an encrypted program or data held in or available to the computer system into readable and understandable format or text, for the purpose of investigating any offence.

Explanation:

This amendment mandates consultation with a qualified cryptologist for decryption tasks. This ensures the involvement of a specialist with the necessary knowledge and experience to manage decryption procedures without compromising data integrity.

Amendment 2: Specialist Involvement in Data Management

The current wording of Section (2)(g):

(g) maintain the integrity of the relevant stored computer data.

New wording:

(g) in consultation with a qualified data management specialist, maintain the integrity of the retrieved and stored computer data.

Explanation:

Similar to the previous amendment, this change requires consultation with a data management specialist when maintaining the integrity of seized data. This ensures that proper procedures are followed to prevent accidental data alteration or loss.

Additional Considerations:

- Amend the bill to include a remedy for data damage.
- Create a definition section within the Act to define terms like "qualified cryptologist" and "qualified data management specialist." This can specify relevant certifications or experience requirements.
- Establish protocols for collaboration between police officers and specialists during investigations.
- Standardization and Certification:
    - Develop a national certification program for police officers demonstrating competency in handling digital evidence. This ensures a minimum level of expertise within law enforcement and promotes best practices.

The proposed amendments aim to create a balance between efficient law enforcement and safeguarding the integrity of digital evidence. By incorporating specialists and enhancing police training, Barbados can strengthen its cybercrime investigation framework while ensuring adherence to legal due process.

Lisa M. Niles <lmniles@arialeeshell.com> 4/26/2024 9:29 AM

Intervention re the Cybercrime Bill (Barbados)

To parliamentbarbados@caribsurf.com

Dear Sirs

Please refer to the attached submission as an intervention to the CyberCrime Bill.

Regards

Lisa N

- Cybercrime Bill - Intervention LN.pdf (4 MB)

April 26, 2024

The Joint Select Standing Committee on Governance
and Policy Matters

Dear Sirs

As a citizen of Barbados, I wish to express my deep concern regarding the Cybercrime Bill.

I am concerned with several sections, the first of which is **Section 19 (3) – Malicious Communication**, which states:

"A person who intentionally uses a computer system to disseminate any image or words, not caring whether ***true*** *or false and causes or is likely to cause or subject a person to ridicule, contempt or embarrassment, is guilty of an offence and is liable on summary conviction to a fine of $70,000 or to imprisonment for a term of 7 years or to both."*

Before I make my submission, I have a query regarding this section: Should this section read a maximum fine and a maximum number of years or is there no discretion in the amount of the fine and the length of imprisonment?

That aside, my major concerns regarding this section of the bill are primarily with the effects which are outlined below:

The chilling effect

The inclusion of the clause, "whether true of false", is problematic. Apart from the foundational issue of the law which is based on the tenets of truth and justice, is this Bill now quelling the revelation or dissemination of truth by computer systems? The belief or even a simple concern that there will be fines or imprisonment as a consequence of truth telling is a deterrent. One only needs to believe they will be embroiled in charges and the consequent publicity regarding the same and this can quell the actions of whistleblowers, those who assist the police and those who advocate for transparency and accountability in public service. The belief alone, is sufficient to have a chilling effect.

The cultural effect

I am concerned about the effect on our culture and the implications for artists. In particular, calypsonians who are able to deliver the truth in witty, rhythmic songs that go on to become a part of history. Unless there is some exception in the Bill, the author, producer, etc. would be subject to a fine of $70,000 or to imprisonment for 7 years or both. "Jean & Dinah" sung by the Mighty Sparrow is a popular old calypso. If the Mighty Sparrow was a Barbadian, and this song embarrassed someone, it seems he could then be subject to the fine and possible imprisonment.

We have seen some imagery from graphic artists and cartoonists that encapsulate the political situation and provide moments of levity. During the 2018 general elections, upon awaking to find out the results of the elections, the first image was of a bus going over a cliff with the faces of the candidates of the Democratic Labour Party. In more recent times, arising from revelations in the budget response to excessive and costly flights by the current administration there was an image of an aircraft and the words MIA Airline, MIA meaning Missing In Action. These images, although about serious matters, allow us to share moments of lightheartedness. They are necessary to keep the political climate one of respectful camaraderie and free from fear. In the thrust and parry of politics, one cannot be so thin-skinned as to criminalise these actions.

The effect on religion

I am further concerned about the effect on religion and the implications for Christians. Do Priests, Elders, Apostles, Eucharistic Ministers and those that address religious congregations, are they now to be mindful of telling the truth and preaching the truth from the pulpit? Will you use the words preached to fine or imprison them and the information technology teams as they live stream?

While these three areas are of grave concern to private citizens that may be subject to charges, is there an exception for politicians and those carrying on government business? Even as this Bill is being debated by the Joint Committee and names of private citizens are referenced and such debate is transmitted via social media... would they too be subject to fines and imprisonment?

Speaking and sharing the truth ought not to be criminalized and on that basis alone, this Bill does not appear to be firmly grounded.

The second section of the Bill I find concerning is **Part 111 – Investigation and Enforcement: Section 23 – Search and seizure.**

This section gives wide authority to police officers. Section 23 (2)(a) states that, in the event of a warrant being issued, a police officer may seize or similarly secure any computer system, data, programme, etc. if he reasonably believes that it is evidence that an offence has been or **is about to be** committed. This language is prospective and seems odd to me, as a layman. The risk of an officer who legitimately believes that a person is about to commit an offence and seizes the computer system, etc. begs the question of what recourse exists if he is incorrect in his belief.

Section 23 (2)(f) appears to be an all-inclusive clause where any other programme or data held in the computer system may be copied and retained. This has serious implications for gatekeepers, programmers, analysts or other legitimate users of the database who are not involved in any criminality. The ripple effect of wide seizure impacts other users.

Recourse or remedy after an injustice perpetrated by application of the law is not a satisfactory standard of law. The language of the law ought to be clear enough to prevent the injustice from occurring under these circumstances.

My final area of concern is **Section 24 – Assisting a police officer.**

This section mandates the provision of assistance to the police and could be in conflict with other areas such as the right to protect proprietary information, non-disclosure agreements, etc. As this Bill is drafted, it seems to me that an expert may be compelled to assist a police officer by virtue of their knowledge of the functioning of a system. Does this contravene human rights?

While these are not my only concerns, these are my primary concerns. In my opinion, as a concerned Barbadian, this Bill should be withdrawn.

Respectfully

Lisa Niles (Miss)

kmk2021biz <kmk2021biz@protonmail.com> 4/26/2024 10:01 AM

Cyber Crime Bill 2023 Section 19 & 20

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Good Morning Sir/Madam,

Below is my submission for the Cyber Crime Bill currently pending

As a law abiding citizen, I find this pending Cyber Crime Bill Section 20 in particular to be unconstitutional, abusive, unlawful and bordering on criminality.
In my humble opinion, it is an over reach of power and breach of privacy if our police service is given authority to retrieve the citizen's electronic devices with no permission granted.
I respectfully submit.

Regards,
Concern Citizen

kgbusiness@caribsurf.com 4/26/2024 11:09 AM

Cyber Crime Proposed Bill 2023

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Good Morning Sir/Madam,

Below is my submission for the Cyber Crime Bill currently pending

As a law abiding citizen, I find this pending Cyber Crime Bill Section 20 in particular to be unconstitutional, abusive, unlawful and bordering on criminality.
In my humble opinion, it is an over reach of power and breach of privacy if our police service is given authority to retrieve the citizen's electronic devices with no permission granted.
I respectfully submit.

Regards,
Concerned Citizen

Doc Weeks

C30

Heather Cole <heathercole66@hotmail.com> 4/26/2024 12:59 PM

To The Clerk of Parliament Comments on the Cybercrime Bill

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

To the Clerk of Parliament

Please find attached comments by citizens of Barbados opposing the Cybercrime Bill. I will be forwarding my own comment later today.

Heather Cole

- Opposing the Cybercrime Bill .docx (29 KB)

SUBMITTED BY: DAVE WEEKES

My Concerns About The Present Content of the Cybercrimes Bill

I believe that in this new world where the computer and other devises permit invisible communicate to and from anywhere in the world, that our government needs to protect its citizens from crimes which we have seen perpetrated online.

We are in favour of having a Cybercrimes Bill. We commend our government on the initiative to have such a Bill. However, as thinking, voting citizens, in reading the Bill there are some clauses which we believe are detrimental to the freedoms we have enjoyed over the years. We wish these section or clauses removed from the bill. These are:

In Section 19(1)(a) the Bill speaks to "Intimidation" as grounds for cyber protection. The truth is that intimidation is an emotional state of mind and occurs daily under normal circumstances in life. Boxers are intimidated by bigger, stronger more experienced boxers, Teachers can be intimidated by a seasoned no-nonsense Principal and the list goes one. In neither of these circumstances is the intimidating Boxer or Principal expected to appear before the law courts and face criminal charges. The law courts themselves are intimidatory in nature. Hence the grounds of "intimidation" as a single pilar of offense needs to be removed from the Bill as a potential for cybercrime.

In Section 19(3) the Bill refers to "ridicule", "contempt" and "embarrassment" as grounds for an offence in cyberworld. I believe again that this is unreasonable, notwithstanding, the extreme punishment of a $70,000 fine or 7 years imprisonment, if found guilty. Ridicule, contempt and embarrassment among other social emotions are facets of normal life and many times, helps us to mature. To use these subjective facets as measures of criminal deviance is extreme and also need to be struck from the Bill.

While the Bill may wish to deal with what it terms "malicious communication" and rightfully so, extreme caution, consultation and due diligence must be completed to ensure the rights and freedoms of citizens are no compromised. I believe, in this context, where the term "malicious" is by nature subjective, that maybe a series of warnings, non-intrusive monitoring and test for consistency of mal-doing be enforced such that the Bill recognizes and is able to establish mal-intent on the part of the perpetrator before criminal charges are brought.

We thank you for this opportunity as a voting citizen of Barbados.

Dave Weekes

SUBMITTED BY: JOCELELENE HINDS

Upon review of the bill, there are several clauses for concern but I wanted to draw specific attention to S. 19(1), (3) as well as 19 (5). These sections are vague and opened to various interpretations. It can therefore be exploited so that persons would be prohibited from speaking freely. The definition of intimidate is subjective and the burden would be shifted to the accused to prove his or her innocence. In my opinion, the judge can only apply an objective approach. A recommendation would be to include an objective test whereby the question is asked "would a reasonable person in a similar situation view the actions as intimidation?

Joycelene Hinds

SUBMITTED BY: TREVOR BLACKMAN

I hereby protest sections of the Cybercrime Bill as a concerned citizen of Barbados. I am a die hearted Bajan. I am not satisfied with the way this government is running the affairs of this country.

SUBMITTED BY: USEPH GREAVES

Bless you, Thought I'd send this message to show support and offer my solidarity with it against the Cybercrime Bill that the government is proposing. Its really crazy in light of what you people fear. All the best.

Useph Greaves

SUBMITTED BY: DEBORAH MARSHALL

I Deborah Marshall is opposed to certain sections of the Cybercrime Bill and I will want it pulled back because it will deny our freedom of Speech in a supposed democratic country.

Deborah Marshall

SUBMITTED BY: Neville

I oppose any section of the Cybercrime Bill that will stop free speech in Barbados.

Neville

SUBMITTED BY: PAULA WALCOTT

My name is Paula Walcott, I do not have a thorough understanding of the Cyber Crime bill, and this also worries me, a lack of public education on this matter. I am also worried about the freedom of speech and the effect this will have on freedom of information, especially online media houses, which are the present and future method of dissemination information. For these reasons, I am against the Cyber Crime Bill.

Paula Walcott

SUBMITTED BY: JOHN MOORE

Petition Against the Cybercrime Bill, 2024
To The Honorable Members of the Barbados Parliament
The citizens of Barbados express a deep concern regarding the proposed Cybercrime Bill, 2024. While recognizing the importance of addressing cyber threats and ensuring digital security, we believe that certain provisions in the bill may have far-reaching implications for individual rights, privacy, and civil liberties.

This bill threatens to infringe upon our rights to privacy, freedom of expression, and access to information online. It could give the government unprecedented power to monitor and control our online activities, potentially leading to censorship and surveillance of innocent citizens.

We urge the government to reconsider this bill and engage in meaningful consultation with stakeholders to develop legislation that upholds both cybersecurity and civil liberties.
Key objections to the bill include:
1. Disproportionate Penalties: The bill imposes severe penalties, including lengthy imprisonment terms for offenses like cyber terrorism. However, the starting point for what entails such acts remains unclear. We ask for clear guidelines to prevent potential abuse of power.
2. Data Privacy Safeguards: The bill lacks adequate safeguards for data privacy. Law enforcement agencies are granted broad powers to access and seize computer data without sufficient protections for individuals' privacy rights.
We respectfully request that the Barbados Parliament reconsider the provisions of the Cybercrime Bill, 2024, and address the concerns raised by the citizens who believe that any legislation enacted should effectively balance national security interests with the protection of civil liberties.
John Moore

SUBMITTED BY: BJORN CLARKE

To whom it may concern. I would like to Oppose the Barbados Cyber Crime Bill section 19 and section 20on the grounds of it can affect the freedom of speech in Barbados. In section 20 the term offensive needs to be properly defined. In that if someone (person A) of a particular political party, religion, or belief system makes a statement and a person (Person B) that opposes that statement will Person A be guilty of an offence. That is not freedom of speech. These sections needs to be removed from the bill.
Bjorn Clarke

SUBMITTED BY: MARGARET POLLARD

Opposition to the Cybercrime Bill 2024. I OPPOSE the CB. primarily secs.19,20 and 24.our last constitution sec. 20 and 21 we have freedom of expression and freedom of assembly consecutively. We cannot afford to be muzzled.

Margaret Pollard

Dave & Marcia <dm_weekes@yahoo.com> 4/26/2024 1:40 PM

SUBMISSION ON THE CYBERCRIME BILL

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Dear Sir/Madame,

I would like to submit my objections to certain sections of the CyberCrime Bill. It is my belief that certain sections of the proposed Barbados cybercrime Bill could be used as an excuse to silence government critics and undermine privacy in Barbados. In many countries of the world with similar cyber law crimes with sections like 19 (i) (iii) (v), 20, already unduly restrict rights and are being used to persecute artists, opposition politician, human rights defenders and religious preachers.

I am therefore asking the government to re-look these sections of the law and ensure that the human rights of Barbadians are not infringed upon.

Marcia Weekes

Thank You,
Dave & Marcia Weekes (Praise Academy & Step By Step Productions)
246-439-7000 (Office)
246-236-7000 (Cell)
516-345-8066 (Magic Jack)
www.praiseacademyofdance.org
Rent or Download our movies @

JOSEPH www.vimeo.com/ondemand/joseph2

Barrow - Freedom Fighter
www.amazon.com/Barrow-Freedom-Fighter-Adrian-Holmes/dp/B088P8TH5D

Vigilante - The Crossing
www.amazon.com/Vigilante-Crossing-Malissa-Alanna/dp/B081KXMJLS

Chrissy www.vimeo.com/ondemand/chrissy

HUSH 2 www.vimeo.com/ondemand/hush2endthesilence

HUSH 3
www.vimeo.com/ondemand/hush3twistedinnocence

HUSH 1 www.vimeo.com/ondemand/hush1

Celia B <cbourne48@hotmail.com> 4/26/2024 4:34 PM

Cybercrime Bill 2024

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Clerk of Parliament

My concern about parts of this Cybercrime bill 2024 is that it intentionally seeks to curb, stifle, hinder public speech and opinion and the dissemination of information.

Criminalization of freedom of expression whether true or false is a dangerous precedent to be set by Government and highly problematic.

Whether you have recourse by law to prove your innocence or guilt is not the issue, the intent of this bill is to curb, stifle and hinder public speech and opinion. Asking people to prove their innocence about something that is true can be burdensome, time consuming, financially draining to the individual and on an already overburden justice system.

Cyber legislation should not be petty, trivial and geared towards people's feelings, this does not belong to any cybercrime legislation especially when these words used in other public spaces are not criminalize.

Barbados needs to recognize that in these modern times a great majority of business and disseminating of information is done online and we must make sure that what we do doesn't prohibit or disadvantage in anyway people's right to live and excel in an evolving cyber space.

Why are we making a human rights issue part of the computer misuse act. Including all these emotional words and feelings are trivial and petty and seeks to defeat the purpose of healthy communication and stops the society from evolving healthily.

Giving power to the security forces to compel people to cooperate with them against their own will in the execution of they duties when they think a crime has or is about to take place is unreasonable. Giving service providers the right to invade one's privacy by sharing one's data without a court order is unacceptable.

Sincerely

Cecilia Bourne

Michael Bourne <mbourne28@gmail.com> 4/26/2024 5:41 PM

Cybercrime bill 2024

To parliamentbarbados@caribsurf.com

To the Clerk of Parliament

I have listened with great interest to the Joint Select Committee –convened on Monday the 22nd April 2024, pertaining to the Cybercrime Bill 2024,in conjunction to reviewing it, focussing primarily on sections 19(5) pertaining to Malicious Communication.

After paying attention to what was said, I am of the opinion that there is an attempt in layman's terms to legalise flimsy insignificant cases, that can easily be misconstrued on all sides, thereby forging an infringement of the right of the Barbadian public to the freedom of expression and the dissemination of information, which to my belief has been intentionally masterminded and orchestrated to criminalise this basic right.

This means, If a comment was made about someone or something relevant that was established to be the truth and that individual was in some way offended or claimed to be emotionally distressed, how do I prove that this was not the intent?

I would like to make reference to a case in Nigeria whereby a pregnant lady faces seven years in jail simply because she said tomato puree was too sweet, as a result she was charged under Section 24(1) (B) of Nigeria's Cyber Crime Prohibition Act, apparently it was the first time she used this product, please see the following links for your perusal as seen below.

A Nigerian woman reviewed some tomato puree online. Now she faces jail | CNN

Nigerian woman faces seven years in prison for writing a damning online review of tomato puree | Daily Mail Online

" Woman faces 7 years in jail for saying tomato puree was too sweet | World News | Metro News

This account, based on this report, is a sad state of affairs and very disconcerting, as it is perceived, a similar trend could be chartering these shores.

This bill is considered to be vindictive, therefore It is my concern that this bill can be manipulated in a manner that may prevent people from voicing opinions and making comments that people in authority could take as offence.

This bill serves absolutely no purpose other than to suppress and control, which is characteristic of a totalitarian nature, it needs to abolished

Kindest Regards
Michael Bourne
Mob:07508222788
Email: mbourne28@gmail.com

theirry gittens <theirrygittensmouri@gmail.com> 4/26/2024 6:39 PM

Oral Presentation Request

To parliamentbarbados@caribsurf.com

Parliament of Barbados,
Parliament Buildings,
Trafalgar Street,
Bridgetown.

Clerk of Parliament,

Dear Sir/Ma'am,

My name is Theirry Gittens, a 21-year-old Computer Science Student at the University of the West Indies. I have written this email in hopes of being given the option to speak on the Cyber Crime Bill and how section 19 subsection 3 negatively affects the youth if that part of the bill is not adjusted. In addition, issues with the amount of the fine being "$70,000" compared to other criminal charges and most importantly the real and immediate danger "Deep Fakes" place our nation in. Thank you in advance for responding to my email as I patiently look forward to your response.

Kind regards,
Theirry Gittens

Lisa Niles <lmichelleniles@gmail.com> 4/26/2024 6:47 PM

Cybercrime Bill and Youth Offenders

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

To the Clerk of Parliament

Please see attached submission for the consideration on the Joint Select Committee on the Cybercrime Bill 2024 regarding implications of the Cybercrime Bill
for youth offenders.

Best regards

--

Lisa M. Niles

***"The time is always right to do the right thing"* Martin Luther King, Jnr.**
"He is no fool who gives what he cannot keep to gain what he cannot lose." Jim Elliott, missionary martyred in Ecuador.

- Submission on Cybercrime Bill and Youth Offenders.pdf (223 KB)

To examine whether the penalties imposed in the Cybercrime Bill as drafted are disproportionate and/or unreasonable in any way.

Section 20 of the Bill entitled "Cyberbullying" imposes a summary conviction to a fine of $70 000 or imprisonment for a term of 7 years or to both.

Approximately one-third of global Internet users are children and adolescents under the age of 18.[1] Childhood and adolescence are crucial periods characterized not only by physical and emotional growth but also by the emergence of risk-taking behaviors. During these stages, young people are particularly vulnerable as they may not fully comprehend the link between their actions and the resulting consequences.
Hence, it's highly probable that a high proportion of offenders falling under section 20 will be underage individuals and youth.
This assertion is supported by statistical data from various regions worldwide.

Research:

- Research in India indicates that 14.5% of teenagers experienced cyberbullying as victims, 5.8% engaged in cyberbullying as offenders, and 13.8% were both victims and offenders. (Indian Journal of Psychiatry, published in 2023[2])
- A UNESCO Fact Sheet reports that based on a study conducted across Australia, Canada, Europe, South Africa, Republic of Korea, and the USA among children aged 11 to 17 years old, nearly 28% reported receiving sexts, approximately 15% admitted to sending sexts themselves, and around 12% acknowledged forwarding a sext they had received **without consent.**[3]
- Comprehensive research spanning 5 years (January 1st, 2015 to December 31st, 2019) on the worldwide incidents of cyberbullying among youth indicates that the frequency of cyberbullying among children and adolescents has notably risen over the past five years, underscoring the urgency for researchers in low and middle-income countries to devote ample focus to this issue.[4]

The case for Restorative Justice:
Considering the significant number of young children engaging with the internet and digital communication platforms, it's essential for the government to contemplate enforcement measures that are suitable for their age. Prioritizing restorative justice principles becomes paramount in ensuring that punitive measures are balanced with opportunities for growth and education, and are aligned with the unique needs and vulnerabilities of young individuals in the digital age.
"*Restorative justice programs offer schools alternative strategies for addressing student misbehavior and complex issues, offer a supportive learning environment conducive to learning, improve student safety, and strengthen connections between students and staff.*" (Akalaonu, 2014, p. 19[5])

The Canadian Standing Senate Committee on Human Rights has recommended "*That the promotion of restorative justice initiatives be a key component of any coordinated strategy to address cyberbullying developed in partnership by the federal, provincial and territorial governments*".

RECOMMENDATION: The penalties outlined in Section 20 of the Cybercrime Bill, as currently drafted, are deemed disproportionate and/or unreasonable, particularly when considering that school-going youth are likely to be the primary offenders. Therefore, it is imperative to substantially revise the Bill to prioritize restorative justice, thereby empowering youth to take responsibility for their actions and facilitating the restoration of harm caused.

References:
[1]UNICEF ed . Children in a Digital World. New York, NY: UNICEF; (2017).
[2]https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10461578/
[3]Tackling cyberbullying and other forms of online violence involving children and young people October 2021 (UNESCO)
[4]Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures
[5]European Forum for Restorative Justice. https://www.euforumrj.org/en/restorative-justice-responses-cyber-harm

Lisa Niles

Lisa Niles <lmichellaniles@gmail.com> 4/26/2024 6:52 PM

Section 20 Cybercrime Bill - Scope, Balance of power and Voidance for vagueness

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

To the Clerk of Parliament

Please see attached submission for the consideration on the Joint Select Committee on the Cybercrime Bill 2024 regarding implications for Scope of Cyberbullying acts, Balance of power and Voidance for vagueness.

Best regards

--

Lisa M. Niles

"The time is always right to do the right thing" Martin Luther King, Jnr.
"He is no fool who gives what he cannot keep to gain what he cannot lose." Jim Elliott, missionary martyred in Ecuador.

- Submission Section 20 Void for Vagueness.pdf (166 KB)

Navigating Language Ambiguity in Section 20 of the Cybercrime Bill 2024: Scope of Acts, Imbalance of power, Voidance for Vagueness

Section 20 of the Cybercrime Bill 2024: Cyberbullying:
The Bill threatens $70,000 fines and/or 7-year incarceration for cyberbullying which includes using a computer system to "*publish, broadcast or transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene...*" or to cause "*annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causing substantial emotional distress...*".

Expanding the scope or meaning of cyberbullying beyond specific definitional terms can lead to challenges in interpretation.
A review of what acts are considered to be cyberbullying in various jurisdictions highlights that the Barbados Cybercrime Bill 2024 unnecessarily broadens the scope of acts of cyberbullying. The Bill uses language that combines words open to being deemed as "vague, overly broad, arbitrary and/or subjective and uncertain" and expands the potential reach of the law beyond what is necessary or clear. This could lead to challenges in enforcement and interpretation, potentially undermining the effectiveness of the legislation in addressing cyberbullying while also raising concerns about the protection of individuals' rights to free expression.

Different jurisdictions define acts of cyberbullying in various ways, but common elements include:

- Harassment: Sending repeated, unwanted messages or threats online.
- Defamation: Spreading false information about someone online that harms their reputation.
- Impersonation: Pretending to be someone else online to deceive or harm others.
- Disclosure of Personal Information: Sharing private or sensitive information about someone without their consent.
- Intimidation: Using fear or coercion to control or manipulate others online.
- Exclusion: Purposefully excluding someone from online communities or activities to isolate or harm them.
- Cyberstalking: Persistently following, monitoring, or harassing someone online.
- Hate Speech: Posting or sharing content that promotes discrimination, hostility, or violence against individuals or groups based on their race, religion, ethnicity, gender, sexuality, or other characteristics.

The focus of cyberbullying typically centers on objectively identifiable behaviors such as hate speech, threats against life, defamation, and extortion. These actions are clear-cut and can be determined based on specific criteria. However, the language used in Section 20 broadens the definition of cyberbullying by encompassing a wider range of expressions. This expansion introduces subjectivity into the determination of what constitutes cyberbullying, potentially leading to inconsistencies and challenges in enforcement and interpretation.

Expanding the scope of individuals who can be victims of bullying or cyberbullying:
Several definitions of bullying (implicitly or explicitly) stipulate that for behavior to qualify as such, it must be repetitive and involve an imbalance of power between the perpetrator and the victim. Bullying or cyberbullying typically occurs when someone with superior physical strength, access to embarrassing information, or popularity uses their advantage to control or harm someone with less power.

Similarly, there exists a potential power disparity between citizens and politicians or law enforcement, typically favoring the latter. Outside of elections, citizens often address this power imbalance through criticism, whether online or offline. However, Section 20 of the Cybercrime Bill potentially penalizes this act of criticism by criminalizing any speech that may cause offense, embarrassment, inconvenience, humiliation, insult, or substantial emotional distress to law enforcement officials or public figures. This

broad language allows any public official to claim offense or distress, thereby silencing legitimate criticism.

This approach fails to acknowledge the inherent power imbalance present in cyberbullying, potentially compromising citizens' ability to exercise their freedom of speech and to comment and criticize anonymously or otherwise.

Subjectiveness of language in Section 20

The interpretation of the terms and phrases within Section 20 of the Cybercrime Bill can vary based on individual perspectives and contexts, leading to ambiguity in their application. Words such as "annoyance", "inconvenience," "offensive," or "substantial" may have different meanings to different people, making it challenging to precisely define the scope of legal provisions.

The language in the Bill therefore provides room for interpretation that may vary among law enforcement officials or judicial bodies and lead to inconsistencies and potential abuse of power in enforcement and legal outcomes. This variance opens the door to disparate treatment of individuals or groups based on subjective understandings of the law. Moreover, in cases where ambiguity exists, there is a risk that those with authority may exploit the uncertainty to justify actions that are not in line with the intended purpose of the Bill.

Vagueness of language in Section 20:

The language used in Section 20 of the Bill carries inherent subjectivity and uncertainty, especially when it falls under the purview of the vagueness doctrine. This legal principle dictates that laws must be clear and specific enough for individuals to understand what conduct is prohibited or required. The vagueness doctrine aims to prevent laws from being so unclear that they fail to provide fair notice to individuals or invite arbitrary enforcement. However, words such as "inconvenience," "offensive," or "substantial" may lack precise definitions, leading to ambiguity in interpretation and render the law unenforceable if it is too vague for the average citizen to understand.

Recommendations for addressing the concerns with Section 20:

- Removal of controversial aspects: Consider removing the more contentious elements of Section 20 to ensure clarity and prevent potential abuse or misinterpretation. Specifically, eliminating language that allows public officials to claim victimhood could prevent misuse of the law for personal or political gain, thereby safeguarding against potential abuse of power and ensuring the fair and impartial application of the legislation.

- Restricting the scope of cyberbullying: Limit the definition of cyberbullying in the Bill to acts that can be defined with specificity, such as hate speech, threats, or defamation, to avoid ambiguity and ensure consistent enforcement. This focused approach will provide clear guidance to law enforcement agencies and the judiciary while still addressing the most egregious forms of cyberbullying.

- Explicitly defining punishable conduct: Clearly and definitively outline what behavior constitutes cyberbullying and is punishable under the law. This will provide clarity to individuals and authorities regarding the boundaries of acceptable online behavior and reduce the risk of the law being deemed void for vagueness.

  By implementing these recommendations, the Committee can enhance the effectiveness and fairness of the Bill aimed at addressing cyberbullying while safeguarding against potential legal challenges.

Lisa Niles

Cindy Benn <benjycindy@gmail.com> 4/26/2024 8:04 PM

Cybercrime Bill, 2024 - Comments

To parliamentbarbados@caribsurf.com

Good evening,

Please see attached document.

Best Regards,
Cindy Benjamin

- Comments Cybercrime Bill 26-4-2024.docx (19 KB)

parliamentbarbados@caribsurf.com

To Whom It May Concern,

Thank you for the opportunity to comment on the Cybercrime Bill, 2024.

I would like to raise concerns I have about certain sections of the bill. They are outlined by section in the schedule below.

Section	Comments
19.(3)	I object to the use of certain language in this section. Terms like 'ridicule' and 'embarrassment', are vague and subject to different interpretations. They should be removed, or replaced by words with more specific meaning.
19.(5)	This provision is troubling. It is very far-reaching and would place an onerous burden on the public in its daily discourse. Barbados has a majority Christian population and in the Bible truth and honesty are treated as virtues. I don't believe someone should be prosecuted for disseminating truthful information that is not private or legally protected.
20.(1) *(b)*	Terms such as 'annoyance', 'inconvenience', 'embarrassment', 'humiliation', 'anxiety', are vague and ambiguous and should be excluded from this section. The protection intended by use of these words is already provided by other terms in this section.
23.(1)	I am troubled by the phrase 'is about to be committed'. The phrase suggests that police officers can read a person's mind, and places them in a position where they are expected to do such. Since in most cases one can never know what another person is about to do, this phrase should be removed.
24.(1)	'A person who fails without lawful excuse or justification to assist a police officer'. This provision is over-reaching and burdensome. It requires an individual to assist a police officer in the carrying out of his or her duties. It places no limitations on the amount of time or degree of assistance that the person is expected to provide.
26.(1)	This section contains provisions that could be dangerous as it has the potential for wide ranging surveillance and monitoring activities. The amount of detailed information that can be requested from telecommunication service providers is over and above what is necessary to identify criminal activity.

Please take these objections into consideration when making any adjustments to the final draft.

Sincerely

26th April, 2024

Philip Corbin <philipcorbin@yahoo.com> 4/26/2024 10:16 PM

FFFB Response to the Proposed Cybercrime Bill 2024

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Attention: Clerk of Parliament.

Please find attached a Submission from Family-Faith-Freedom, Barbados re the Proposed Cybercrime Bill.

Regards

Dr. Philip Corbin
Chairman, FFFB
26 April, 2024

- FFFB Response to the Proposed 2024 Cybercrime Bill.pdf (273 KB)

Family-Faith-Freedom, Barbados (FFFB) Response to the Proposed 2024 Cybercrime Bill

The principal object of Family-Faith-Freedom, Barbados (FFFB) is to promote family, faith and freedom in Barbados based on the principles of the Kingdom of God and in accordance with our Statement of Faith, as expressed in the FFFB Constitution. In line with this, one purpose of FFFB is to endeavour to influence public policy and government legislation through research and advocacy on personal freedom, family values, God-given rights and empowerment, child survival and protection of human life from conception till natural death.

While FFFB lauds the sections of the Cybercrime Bill that seek to suppress child pornography, child grooming, and online child sexual abuse, we believe that the Bill in its current form lends itself to undermining the fundamental human rights of freedom of conscience and freedom of expression.

Consider the following possible, true-to life scenarios that the Bill could engender if passed:

1. A future "Gabby", call him G, makes a future musical "hit" about a future "Jack", call him J. Under the "Malicious Communications" section of this Cybercrime Bill, in particular Subsections 19 (1) a, and 19 (4), J could bring a lawsuit against G, and G could be facing a fine of $70,000 Bds or 7 years in prison.

2. A truth is electronically circulated from person A concerning person B, which person B finds personally offensive. B could use Section 20 of the Cybercrime Bill, on cyberbullying, to bring a lawsuit against person A, irrespective of whether what A said is true or provable. The computer of A could be seized for an indefinite period, and, as in the case of G above, he or she could be facing a fine of $70,000 Bds or 7 years in prison.

3. Even if eventually legally exonerated, characters G and A could be severely affected in their livelihoods, both through the damage to their reputations, legal costs fighting the lawsuits, and the removal of their computer equipment for an extended period. The Bill does not even say for how long A's computer equipment would be seized, or if, or how, G would be compensated for his financial losses.

4. Further, if characters G or A received help from others in their song or writings, then according to Section 22 of the Cybercrime Bill, those "aiding and abetting" G or A could likewise be facing fines of $70,000 Bds or 7 years in prison. Such scenarios should have no place in our new republic.

The Cybercrime Bill has much potential value, and care must be taken to craft it as a positive contribution to a better Barbados. Words have power. Language is a powerful tool that can be manipulated, sometimes even with a subconscious intentionality. It is therefore important to ensure that the Bill avoid the use of words and phrases that have, in other jurisdictions, lent themselves to unjust litigious ends. As a case in point, consider Clause 20.(1) of the Bill. In its current form, the Clause threatens the fundamental right to freedom of expression; a violation which has no right in a democratic society.

Consider the Clause as it currently stands, and compare it with the following revised version by a policy analyst who has a background in digital and analogue technology:

Current Clause: *"A person who intentionally uses a computer system to publish, broadcast or transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene or of a menacing character or causes any such data to be so sent; for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress to that person, is guilty of an offence and is liable on summary conviction to a fine of $70,000 or to imprisonment for a term of seven years or to both."*

Suggested revision: *"A person who intentionally uses a computer system or a similar digital or analogue device or system to publish, print, broadcast or transmit data that is defamatory or fraudulent, pornographic, obscene or of a menacing or bullying character or actively causes such data to be so sent with malicious, tortuous or criminal intent for the purpose of causing defamation, slander or libel, malicious endangerment, unlawful obstruction, interference with lawful contracts, business or employment, significant risk of, or actual physical or emotional injury, intimidation or incitement, is guilty of an offence and is liable on summary conviction to a fine of $70,000 or to imprisonment for a term of seven years or to both."*

The suggested revision uses no emotionally-charged language and therefore has fewer subjective elements that can lead to self-serving interpretations.

Family-Faith-Freedom, Barbados recommends that this new Cybercrime Bill be taken back to the drawing board, retaining its positive elements, but being careful to address, practically and efficiently, those aspects of cybercrime that were not included in the Computer Misuse Act.

Submitted by:
Dr. Philip Corbin
Chairman, FFFB
26 April, 2024

To The Clerk of Parliament

Comment on the Cybercrime Bill 2024

SUBMITTED BY: CARLYLE SYLVESTER EDWARDS

As a citizen of this country I feel that we the people should have good claim of right to object to the Cybercrime Bill. We did not vote for you to treat us like last week's garbage. We need you to seriously respect us!

Carlyle Sylvester Edwards

Heather Cole <heathercole66@hotmail.com> 4/26/2024 11:26 PM

To the Clerk of Parliament Comment on Cybercrime Bill

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

To the Clerk of Parliament

Please find attached comments of Carlyle Edwards opposing the Cybercrime Bill.

- cybercrime submission of cedwards.docx (18 KB)

C39

Kally B <kallertz62@gmail.com>

4/26/2024 11:55 PM

Cybercrime Bill, 2024- Submission

To parliamentbarbados@caribsurf.com

This mail has no content

- Cybercrime Bill. 2024.docx (22 KB)

Concerns related the Cybercrime Bill, 2024

I write to declare that I stand against this Bill in its present form as I believe it may infringe on and even criminalise freedom of speech of Barbadians.

Among many other deficiencies, part II 19.(1) of this legislation imposes a fine of $70,000 and 7 years of imprisonment for transmitting computer data that "intimidates a person" even if the data is completely factual and in the public interest. Additionally part II 20.(1) criminalises speech that is deemed "offensive" and causes "anxiety" or "emotional distress".

This vague language poses significant challenges as it can be used indiscriminately to curb freedom of expression and be leveraged to silence criticisms of politicians/public personalities, shield politicians from accountability, or even facilitate unjust political persecution.

Illegal Access

Part 11 (4) (1-2) is overly broad and risks implicating innocent individuals like cybersecurity professionals, researchers, activists, and whistleblowers. Without proper training for judicial officers to differentiate between criminal acts and actions serving the public good or enhancing cybersecurity practices, it becomes even more problematic. Qualifiers must be incorporated into legislation to differentiate acceptable behaviours from criminal ones, safeguarding those who work for the public good.

Search and seizure

Part III (23) (1-2) gives law enforcement excessively broad powers when it comes to confiscation and access to computer systems (including smaller form factors such as tablets and mobile phones). These types of powers require independent and effective oversight functions (as does this entire Act).

Production of data for criminal proceedings

Part III (26) (1) This gives law enforcement excessively broad and intrusive surveillance powers when it comes to intercepting Internet communications, compelling service providers to handover subscriber data and Internet activity, and other potentially disproportionate collection or interception of online communications. These types of powers require independent and effective oversight functions (as does this entire Act). Again, the oath of a police officer shouldn't be enough to obtain a warrant that allows for such intrusive acts.

I encourage government to heed to well-informed expert advice and the genuine concerns of many citizens and revise this legislation.

Lisa Niles <lmichelleniles@gmail.com> 4/26/2024 11:58 PM

Signatures to Petition

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Dear Clerk of Parliament

This submission is in the form of a petition signed electronically.
The attached list of persons have signed to the CHANGE.ORG petition regarding amending the Cybercrime Bill 2024.

- CHANGE.ORG PETITION SIGNATURES.pdf (257 KB)

Petition to:

Amend the Barbados Cybercrime Bill 2024 & Remove the risk of human rights violation

In recognition of the fundamental principles established by the Human Rights Council of the United Nations, including its consistent reaffirmation that the "*same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice,*" **we, the undersigned, advocate for the review and amendment of specific articles within the Cybercrime Bill 2024.**

We emphasize the importance of involving the public in this process. Below, we outline our concerns and comments regarding the Cybercrime Bill 2023:

CONCERNS:

Broad Powers: The Cybercrime Bill grants courts and law enforcement extensive authority to seize individuals' computer devices and compel access under threat of charges for non-compliance.
Telecommunication Company Compliance: It allows courts and law enforcement to compel telecom companies like Digicel or Flow to provide location data from cell towers, Internet browsing activity, and metadata from phone calls without sufficient legal justification.
Privacy breaches and the risk of data misuse: Telecommunication Companies can be mandated to retain and archive customer usage data, including information facilitating user identification, details regarding the content of information systems, and data associated with the equipment utilized. These Companies can possess comprehensive records of all user activities, encompassing phone calls, text messages, visited websites, and applications accessed on smartphones and computers.

Harsh Penalties: Offenses under the bill carry hefty fines up to $70,000 and/or 7 years of incarceration. This includes using a computer system to transmit offensive or indecent data, causing annoyance, inconvenience, danger, or substantial emotional distress.
Ambiguity: The vague definition of prohibited acts such as publishing, broadcasting or transmitting data that is *"offensive, pornographic, indecent, vulgar, profane, obscene..."* or that causes *"annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causing substantial emotional distress... "* poses a risk of abuse of power and miscarriages of justice, potentially undermining fairness and due process in the legal system.
Surveillance Society: The provisions in the Bill have the potential to contribute to a surveillance society by enabling widespread misuse and abuse of personal data.
Government Surveillance Authority: The Bill grants the government significant surveillance authority without adequate checks and balances to prevent potential law enforcement overreach.
International Standards: To address these issues, the Bill should align with Article 15 of the Budapest Convention, which requires conditions and safeguards for the adequate protection of

human rights and liberties.
Oversight Mechanisms: Oversight could be improved by implementing impartial tribunals, appellate courts, or specialized judicial bodies to review and regulate the implementation of the Bill's provisions.

REAL-LIFE Examples of Abuse of Cyber Freedom:

Human rights advocates globally confront increased arrests and convictions, representing a severe assault on freedom of expression. Cybercrime laws, with their broad and unclear and ambiguous provisions, empower governments to suppress dissent by controlling information. Bloggers and journalists are targeted, facing harsh penalties, including lengthy prison terms of up to 10 years, solely for their online activities and expressions, under accusations of spreading misleading or offensive content.

Below are **real-life examples of human rights violations** and infringements on freedoms enabled by cybercrime legislation, reminiscent of the potential deficiencies found in the Barbados Cybercrime Bill:

Abuja, Nigeria: A Nigerian woman who wrote an online review of a can of tomato puree is facing imprisonment after its manufacturer accused her of making a "malicious allegation" that damaged its business. Her review was: "*Help me advise your brother to stop ki***ing people with his product, yesterday was my first time of using and it's pure sugar.*" A week later, on September 24, she was arrested.

Senegal: June 2023: The Senegalese government implemented curfew-like internet shutdowns, effectively restricting access from 1 p.m. to 2 a.m. nationwide. This measure was allegedly aimed at suppressing dissent surrounding the trial of opposition figure Ousmane Sonko.

West Bank, Palestine: The June 2017 cybercrime legislation includes ambiguous terms and principles that Palestinian authorities can exploit with ease. Notably, Articles 16, 20, and 51 include fines or imprisonment, under vaguely defined offenses like "*endangering the security and integrity of the State*" and "*instigating racial tensions and undermining national unity.*" The enforcement of the law in 2017 led to the arrest of numerous journalists and activists, such as Ahmed Awartani and Ibrahim al-Masri, before subsequent modifications were made. Palestinian Independent Commission for Human Rights has said of the Cybercrime law in Palestine: that it is "*a big setback to the freedoms in the West Bank*".

Libya: Human Rights Watch warn that the 2022 Anti-Cybercrime Law restricts freedoms of speech. February, 2023, Libyan authorities detained a female singer and an online content creator, accusing them of breaching the law and transgressing "honor and public morals."

Egypt: The Cybercrime Law allows for the prosecution of individuals on vague grounds such as "threatening national security," "undermining family values," or "affecting public morals," without offering precise definitions of these offenses. Example: Armed police officers raided the

home of Wael Abbas, an acclaimed journalist and advocate for human rights. Without producing an arrest warrant, they blindfolded him and escorted him, still in his pajamas, to an undisclosed location. The law enables the government to block websites infringing upon freedom of expression rights.

Bahrain: The Cybercrime law grants multiple government bodies, the authority to block and censor a broad spectrum of websites. There's no requirement for a court order to censor websites hosting content perceived as a "challenge" to the government. This includes any material critical of the Bahraini government, the royal family, or the prevailing status quo, as evidenced by the situation surrounding the Al-Wasat newspaper.

These actions are inconsistent with the Universal Declaration of Human Rights which explicitly guarantees freedom of thought and opinion. According to this Declaration, all individuals possess the right to express their opinions through various mediums, including speech, writing, pictures, or any other form of expression and publication.

CALL TO ACTION TO THE BARBADOS GOVERNMENT :

In alignment with the United Nations Human Rights Committee's General Comment No. 34 (2011) on Article 19: Freedoms of Opinion and Expression, we call upon the Government of Barbados to amend the Cybercrime Bill 2024 in order to:

- Eliminate ambiguity and provide clear definitions for offenses deemed punishable. Clearly define "*offensive, pornographic, indecent, vulgar, profane, obscene...*" and "*annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causing substantial emotional distress*" to prevent unnecessary or disproportionate interference with freedom of expression.
- Avoid excessive restrictions on access to information.
- Prevent the stifling of freedom of expression.
- Avoid excessively punitive measures and penalties.
- Establish independent checks and balances to mitigate the risk of human rights violations.
- Not discriminate in favor of or against specific religions or belief systems, their adherents, or religious believers over non-believers.
- Prohibit the prevention or punishing of criticism of religious leaders or commentary on religious doctrine and tenets of faith.
- Protect all forms of opinion, including political, scientific, historic, moral, or religious opinions, as criminalizing holding an opinion is incompatible with Article 19 (1).
- Implement and uphold laws safeguarding citizens' privacy rights.
- Avoid the harassment, intimidation, or stigmatization of individuals for their opinions, including arrest, detention, trial, or imprisonment, as this constitutes a violation of Article 19 of the Universal Declaration of Human Rights.
- Ensure public involvement in its revision and amendment.

ELECTRONIC SIGNATURES

Name	Country	Signed On
Sonia Ashby-King	Barbados	2024-04-22
Valerie Hoyte	US	2024-04-22
Patricia Cox	Barbados	2024-04-22
Heather Cole	US	2024-04-22
Sue Harris	US	2024-04-22
Mervin Marius	Barbados	2024-04-22
Joyann Welch	Barbados	2024-04-22
D Reece	Barbados	2024-04-22
Marietta Forde	US	2024-04-22
Jeanie Mottley	Barbados	2024-04-22
Carolyn Howard	Barbados	2024-04-22
Janette Carter Godman	US	2024-04-22
Jennifer Fields	Barbados	2024-04-22
Sonia Perch	Barbados	2024-04-22
Michelle Alleyne	US	2024-04-22
David Bailey	Barbados	2024-04-22
Andora Goodman	Barbados	2024-04-22
Genefer Pile	Barbados	2024-04-22
Alice Murray	Barbados	2024-04-22
Carolyn Drayton	Barbados	2024-04-22
Paul Massiah	Barbados	2024-04-22
Emmerson Babb	UK	2024-04-22
Calvin Barker	UK	2024-04-22
Tracey Barrow	Barbados	2024-04-22
C. St. Clair Browne	Barbados	2024-04-22
Hugh Greene	Barbados	2024-04-22
Elise Layne	Barbados	2024-04-22
fred corbin	Barbados	2024-04-22
Jasmine Adams	Barbados	2024-04-22
Cheryl Gibson	Barbados	2024-04-22
Virginia Clarke	Barbados	2024-04-22
Shawn Tudor	Barbados	2024-04-22
Tyrone Nurse	Canada	2024-04-22
Juel King	Barbados	2024-04-22
Chazayah Pitt	Barbados	2024-04-22
Christelle A King	Barbados	2024-04-22
Rogerio Mayers	Barbados	2024-04-22

Beverly Brathwaite	Barbados	2024-04-22
Adrian Brome	Barbados	2024-04-22
Cheryl Clarke	Barbados	2024-04-22
David Weekes	US	2024-04-22
P Sandra Hinds	Barbados	2024-04-22
Alvin Barker	Barbados	2024-04-22
Lisa Niles	Barbados	2024-04-22
Noel Welch	Barbados	2024-04-22
Paula Walcott	Barbados	2024-04-22
Karen Walcott	Barbados	2024-04-22
Sylvanus Nicholas	Barbados	2024-04-22
Jackie Evelyn	Barbados	2024-04-22
Julia Nicholls	Barbados	2024-04-22
Althea Yarde	Barbados	2024-04-22
Leonard Jones	Barbados	2024-04-22
Laura Worrell	Barbados	2024-04-22
Hugh Shepherd	Barbados	2024-04-22
John Moore	Barbados	2024-04-22
Jennifer Edwards	Barbados	2024-04-22
Ronald Webster	Barbados	2024-04-22
Cyralene Murray	Canada	2024-04-22
Orville Brathwaite	Barbados	2024-04-22
Keith Kinch	Barbados	2024-04-22
Mark Gibling	Barbados	2024-04-22
Rosemarie Layne	Barbados	2024-04-22
Dave Layne	Barbados	2024-04-22
Annaliese Bayne	Barbados	2024-04-22
Jane Scott	Barbados	2024-04-22
Wayne Marshall	Barbados	2024-04-22
Nem Maxwell	US	2024-04-22
Belfield Belgrave	Barbados	2024-04-22
Hugh Shepherd	Barbados	2024-04-22
John wayne Scantlebury	Barbados	2024-04-22
Lori Arnold	US	2024-04-22
Alicia Lorde	Barbados	2024-04-22
Esther Gooding	Barbados	2024-04-22
Sophia Clarke	Barbados	2024-04-22
Lennox Wiggins	Barbados	2024-04-22
Sheldon Mottley	US	2024-04-22
Peter Earle	Barbados	2024-04-22

LOMA GITTENS	Barbados	2024-04-22
Lee Gill	Barbados	2024-04-22
Jason Bynoe	Barbados	2024-04-22
Sylvan Greenidge	Barbados	2024-04-22
Adrian Marshall	Barbados	2024-04-22
Eric Smith	Barbados	2024-04-22
David Clarke	Barbados	2024-04-22
Jacqueline Ward	Barbados	2024-04-22
Dora Franco	Barbados	2024-04-22
Gina Denny	Barbados	2024-04-22
Richard Mayers	US	2024-04-22
Terry Carrington	Barbados	2024-04-22
Aveline Mottley	Barbados	2024-04-22
Christopher Carter	US	2024-04-22
Bonnie Springer	Barbados	2024-04-22
Lucinda Alleyne	Barbados	2024-04-22
Marcia Taylor	Barbados	2024-04-22
Dorial Clarke	Barbados	2024-04-22
Natasha Wilson	Barbados	2024-04-22
Maria Annel	Barbados	2024-04-22
Hazel Murray	US	2024-04-22
zach small	Barbados	2024-04-23
Gaymel Jenkins	Barbados	2024-04-23
Everton Hunte	Barbados	2024-04-23
Marlyn Pinnock	US	2024-04-23
Annemarie Forde	Barbados	2024-04-23
Trevor Lynch	Barbados	2024-04-23
Jasmine Maloney	Barbados	2024-04-23
Judiet Harding	Barbados	2024-04-23
Colin Roach	Barbados	2024-04-23
Jonlyn Harewood	Barbados	2024-04-23
Cecil Clarke	Barbados	2024-04-23
Jeremiah Joseph	Barbados	2024-04-23
Anthony Hassell	Barbados	2024-04-23
Sharon Brandford	Barbados	2024-04-23
Vanessa Mansfield	Barbados	2024-04-23
Dale Murrell	Barbados	2024-04-23
jacynthia green	Barbados	2024-04-23
Dave Weekes	Barbados	2024-04-23
Merlene Skeete	Barbados	2024-04-23

Alma Worrell	Barbados	2024-04-23
Levar Greaves	Barbados	2024-04-23
Judith-Ann Clarke	Barbados	2024-04-23
Nelly Risbrook-Wiltshire	Barbados	2024-04-23
Doriel Gamble	Barbados	2024-04-23
Junior Welch	Barbados	2024-04-23
Cecilia Millar	Barbados	2024-04-23
Treavy Price	Barbados	2024-04-23
S Clarke	Barbados	2024-04-23
Edward Tull	Barbados	2024-04-23
NOEL Browne	US	2024-04-23
Yvette Small	Barbados	2024-04-23
Lemuel Tull	Barbados	2024-04-23
Pauline Maynard	US	2024-04-23
Ilene Tull	Barbados	2024-04-23
Swahali Jemmott	Barbados	2024-04-23
Alfred Pope	Barbados	2024-04-23
Monica Hoyte	Barbados	2024-04-23
Carol Barker	Barbados	2024-04-23
Jamila Haywood	Barbados	2024-04-23
Glendene Dottin	Barbados	2024-04-23
VERNON GARNES	US	2024-04-23
Charmaine Hunte	Barbados	2024-04-23
Fred Walcott	Barbados	2024-04-23
Kent Clarke	Barbados	2024-04-23
Jerome Goodman	US	2024-04-23
Catherine Springer	Barbados	2024-04-23
Sharon Cain	Barbados	2024-04-23
Jo-anne Tull	Trinidad & Tobago	2024-04-23
Andy Yearwood	Barbados	2024-04-23
Hugh Clarke	Barbados	2024-04-23
Moshe Gittens	US	2024-04-23
Jacqueline Robinson	Canada	2024-04-23
Adrian Hinds	US	2024-04-23
Mazie Taylor	Barbados	2024-04-23
Bernard Pooler	Barbados	2024-04-23
Ricardine Gibbons	Barbados	2024-04-23
Sharon Belle	Barbados	2024-04-23
Wayne Crichlow	Barbados	2024-04-23

Stephenson Carter	Barbados	2024-04-23
glendon belle	Barbados	2024-04-23
Euna King	Barbados	2024-04-23
Jacqueline Alleyne	Barbados	2024-04-23
Betty Haynes	US	2024-04-23
Victor Lewis	Barbados	2024-04-23
Don Alleyne	US	2024-04-23
Glenn Holder	Barbados	2024-04-23
Dalton Medford	Barbados	2024-04-23
Michelle Ward	Barbados	2024-04-23
Marcia Welch	Barbados	2024-04-23
andy hoyte	Barbados	2024-04-23
June Babb	Barbados	2024-04-23
Diana Babb	Canada	2024-04-23
Sonia Belgrave	US	2024-04-23
Clive Osbourne	Barbados	2024-04-23
Alexander Corbin	Barbados	2024-04-23
Stephen Jackman	Barbados	2024-04-23
Llewellyn Bovell	Barbados	2024-04-23
Angela Clarke	Barbados	2024-04-23
Malcolm Hunte	Barbados	2024-04-23
Marleen Knight	Barbados	2024-04-23
Ricardo Grant	Barbados	2024-04-23
Marcia Chandler	Barbados	2024-04-23
Peter Thompson	Barbados	2024-04-23
Ronald Greenidge	Barbados	2024-04-23
Matthew King	Barbados	2024-04-23
Dwayne Freeman	Barbados	2024-04-23
Victor Benn	Barbados	2024-04-23
Selastine Farmer-Belgrave	Barbados	2024-04-23
Dexter Smith	Barbados	2024-04-23
James Goddard	Barbados	2024-04-23
Paula Brooker	Barbados	2024-04-23
Sherri Cox	Barbados	2024-04-23
Tricia Sealy	Barbados	2024-04-23
Hazel Brathwaite	Barbados	2024-04-23
Jude Young	Barbados	2024-04-23
Sonia Adamson	Barbados	2024-04-23
Aaron Paul	Barbados	2024-04-23

Shalem Evangelical Church	Barbados	2024-04-23
Eunice Greaves	Barbados	2024-04-23
Chinere Phillips	Barbados	2024-04-23
Kevin Chase	Barbados	2024-04-23
Annette Campbell	Barbados	2024-04-23
Aubrey Oneale	Barbados	2024-04-23
PETER CARTER	Barbados	2024-04-23
Lisa Cheeseman	Barbados	2024-04-23
Michelle Harewood	Barbados	2024-04-23
Dr Vonie Austin-James	US	2024-04-23
Raghunanan Jankee	Trinidad & Tobago	2024-04-23
Anthony Hinkson	Barbados	2024-04-23
Ian Gale	Barbados	2024-04-23
Gladstone Hazel	U.S. Virgin Islands	2024-04-23
Norm Black	Barbados	2024-04-23
Edgar Small	Barbados	2024-04-23
Pauline Holder	Barbados	2024-04-23
Risa Niles	Canada	2024-04-23
Roland Waithe	Barbados	2024-04-23
Vernon Dehaney	Barbados	2024-04-23
Keith Lynch	Barbados	2024-04-23
Erwin Bradshaw	Barbados	2024-04-23
Patricia Gulstone	Barbados	2024-04-24
Kimberley Wiggins	Barbados	2024-04-24
Victor Hunte	Barbados	2024-04-24
Merlin Myers	Barbados	2024-04-24
Amanda Campbell	Barbados	2024-04-24
Glyne Murray	Barbados	2024-04-24
Neil S	Barbados	2024-04-24
Tori Layne	Barbados	2024-04-24
Wayne CAMPBELL	Barbados	2024-04-24
John Carter	Barbados	2024-04-24
Millicent Holder	Barbados	2024-04-24
Henderson Bynoe	Barbados	2024-04-24
Emily Callender	Barbados	2024-04-24
Marcie Weekes	Canada	2024-04-24
Anthony Carter	Barbados	2024-04-24
Rich Prosper	Barbados	2024-04-24

John Rogers	Barbados	2024-04-24
Adrian Gibbs	Barbados	2024-04-24
Pamela Hunte	Canada	2024-04-24
Angela Reade	Barbados	2024-04-24
Heather Morris	Barbados	2024-04-24
Rae Reade	Barbados	2024-04-24
John nurse	Barbados	2024-04-24
Leonard Payne	Barbados	2024-04-24
Barbara Weekes	Barbados	2024-04-24
Dianna Springer-Foster	Barbados	2024-04-25
Avery Rudder	Barbados	2024-04-25
Whyvonna Wiggins-Hoyte	Barbados	2024-04-25
Prince Bayley	Barbados	2024-04-25
Irene Holder	Barbados	2024-04-25
W Wiggins	Barbados	2024-04-25
James Prosper	Barbados	2024-04-25
Sarrah Durrant	Barbados	2024-04-25
Sharon Price	US	2024-04-25
Karen Deane-Phillips	Barbados	2024-04-25
Allison Aimes	Barbados	2024-04-25
Hanna R	Barbados	2024-04-26
Steve Skeete	Barbados	2024-04-26
Andrew Price	Barbados	2024-04-26
Jillian Clarke	Barbados	2024-04-26
Michelle Hinds	Barbados	2024-04-26
Marcia Weekes	Barbados	2024-04-26
Maegaret Harris	Barbados	2024-04-26
Christopher Smart	Barbados	2024-04-26
Jacqueline Celeste Carter	Barbados	2024-04-26
Nigel Newton	Barbados	2024-04-26
Valerie Thorpe	Barbados	2024-04-26
Lorraine Sealy	Barbados	2024-04-26
Julia Blenman	Barbados	2024-04-26
Michael Cummins	Barbados	2024-04-26
K L	Barbados	2024-04-26
Jason Collymore	Barbados	2024-04-26
Anthony Bynoe	Barbados	2024-04-26
Krys May	Barbados	2024-04-26
Sherryann Springer	Barbados	2024-04-27

Celia B <cbourne48@hotmail.com> 4/27/2024 12:42 PM

Fw: "Erratum" Cybercrime Bill 2024

To parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>

Clerk of Parliament

Please see attached my submission correcting an error in the submission of Cybercrime Bill 2024 previously transmitted to you on 26th April 2024. The correction is set out in my revised submission in red. Please confirm receipt of this email.

My concern about parts of this Cybercrime bill 2024 is that it intentionally seeks to curb, stifle, hinder public speech and opinion and the dissemination of information.

Criminalization of freedom of expression whether true or false is a dangerous precedent to be set by Government and highly problematic.

Whether you have recourse by law to prove your innocence or guilt is not the issue, the intent of this bill is to curb, stifle and hinder public speech and opinion. Asking people to prove their innocence about something that is true can be burdensome, time consuming, financially draining to the individual and on an already overburden justice system.

Cyber legislation should not be petty, trivial and geared towards people's feelings, this does not belong to any cybercrime legislation especially when these words used in other public spaces are not criminalize.

Barbados needs to recognize that in these modern times a great majority of business and disseminating of information is done online and we must make sure that what we do doesn't prohibit or disadvantage in anyway people's right to live and excel in an evolving cyber space.

Why are we making a human rights issue part of the computer misuse act. Including all these emotional words and feelings are trivial and petty and seeks to defeat the purpose of healthy communication and stops the society from evolving healthily.

Giving power to the security forces to compel people to cooperate with them against their own will in the execution of they duties when they think a crime has or is about to take place is unreasonable.

I am also concerned that service providers can be ordered to share a customer's data with the police without informing the customer, and without any protection of that information or the customer's privacy. There are not sufficient protections for Barbados citizens and voters against police abuse of the very wide powers given to them under the Investigation and Enforcement provisions of the Bill.

Sincerely
Cecilia Bourne

From: Celia B <cbourne48@hotmail.com>
Sent: Friday, April 26, 2024 8:34 PM
To: parliamentbarbados@caribsurf.com <parliamentbarbados@caribsurf.com>
Subject: Cybercrime Bill 2024

Clerk of Parliament

My concern about parts of this Cybercrime bill 2024 is that it intentionally seeks to curb, stifle, hinder public speech and opinion and the dissemination of information.

Criminalization of freedom of expression whether true or false is a dangerous precedent to be set by Government and highly problematic.

Whether you have recourse by law to prove your innocence or guilt is not the issue, the intent of this bill is to curb, stifle and hinder public speech and opinion. Asking people to prove their innocence about something that is true can be burdensome, time consuming, financially draining to the individual and on an already overburden justice system.

Cyber legislation should not be petty, trivial and geared towards people's feelings, this does not belong to any cybercrime legislation especially when these words used in other public spaces are not criminalize.

Barbados needs to recognize that in these modern times a great majority of business and disseminating of information is done online and we must make sure that what we do doesn't prohibit or disadvantage in anyway people's right to live and excel in an evolving cyber space.

Why are we making a human rights issue part of the computer misuse act. Including all these emotional words and feelings are trivial and petty and seeks to defeat the purpose of healthy communication and stops the society from evolving healthily.

Giving power to the security forces to compel people to cooperate with them against their own will in the execution of they duties when they think a crime has or is about to take place is unreasonable. Giving service providers the right to invade one's privacy by sharing one's data without a court order is unacceptable.

Sincerely
Cecilia Bourne

THE BARBADOS POLICE SERVICE

OFFICE OF THE COMMISSIONER

BRIDGETOWN

PUBLIC SECTOR REFORM
Making Barbados Work Better

All Correspondence to be Addressed: -

THE COMMISSIONER OF POLICE
P.O. BOX 84
BRIDGETOWN,
BARBADOS
WEST INDIES.

Ref. No......37/24/1/6.....

April 30, 2024

Mr. Pedro Eastmond
Clerk of Parliament
Parliament
Parliament Buildings
BRIDGETOWN

Dear Sir

Cybercrime Bill, 2024
Mutual Assistance in Criminal Matters (Amendment) Bill, 2024

I refer your correspondence dated April 15, 2024 on the subject at caption and received at the Office of the Commissioner of Police on April 23, 2024.

Following are the comments of The Barbados Police Service:

Apropos the Cybercrime Bill, 2024, on review it demonstrates compliance with the provisions outlined within the Budapest Convention. The Budapest Convention is the international gold standard that all countries in drafting Cybercrime laws must mirror their provisions to ensure best practices. The Cyber Bill has followed the articles which create the offences which combat Cybercrime. Of note, two offences namely the Malicious Communications at Section 19 and Cyber Bullying at Section 20 which have caused much public debate have been amended. I will therefore only focus on those two sections in detail.

The offence of Malicious Communications as captured at Section 19 of the Bill is an offence which was previously featured at Section 14 of the 2005 Computer Misuse Act, Cap 124B, which over time

became outdated. The provisions found within the newly defined offence in the Cybercrime Bill 2024 makes provisions to reflect the changing behaviour of persons misusing computer systems to perpetuate cybercrimes. For example, the Bill creates the offence of revenge pornography at subsection 19(2)(a).

The offence of Malicious Communications under Section 19 of the 2024 Bill, unlike section 14 of the Computer Misuse Act, Cap. 124B attracts very severe penalties ranging from 7 years imprisonment upon summary conviction or a fine of $70,000.00 or to both. This new approach to this offence, reflects that the drafters consider this offence as troubling within our modern society and wants to send the most serious message to would-be offenders. From a law enforcement perspective, the new provisions make it easier for law enforcement officers to investigate cyber-related matters reported to the police.

The offence of Cyber bullying found at Section 20 of the Cybercrime Bill, 2024 is a new offence. The provisions in this new offence are similar to those captured in the offence of Malicious Communications at Section 19 of the Cybercrime Bill, 2024. As with the offence under Section 19, this offence of cyber bullying attracts severe penalties ranging from 7 years imprisonment upon summary conviction or a fine of $70,000.00 or to both. Similarly, with the offence of Malicious Communications, the provisions of this offence make the job of law enforcement officers much simpler to deal with since the provisions are modern and more relevant. Both offences can be dealt with in the Magistrates Court.

Finally, I note that the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024 contains provisions that recognise the need for cooperation between states and private industry in combatting cybercrime. These provisions recognise the need to protect legitimate interests in the development and use of new technologies. They seem proportionate and adequate recognising that the fight against cybercrime requires speed, agility, and co-operation in criminal matters. These provisions comport with the articles 25-34 contained in the Budapest Convention.

RICHARD A. BOYCE
Commissioner of Police

Octave

Submission to the Joint Select Committee (Standing) on the Cybercrime Bill

Presented by Niel Harper

6 May 2024

Presenter Bio - Niel Harper

Cybersecurity & Cybercrime || Digital Policy || Technology Management || Corporate Governance

Relevant Qualifications:

Master of Laws (LLM), Internet Law & Policy – Specialization in Cybercrime, Privacy & National Security ***(University of Strathclyde)***
Postgraduate Diploma (PgD), Telecoms Regulation & Policy ***(University of the West Indies)***
Executive Certificate, Cybersecurity Strategy & Leadership ***(Florida International University - Organisation of American States)***
Certificate, Fintech Law & Policy ***(Duke University)***
Certificate, Internet Governance & Policy ***(University of Malta - DiploFoundation)***
Certificate, Internet Governance & Policy - Cybersecurity ***(University of Malta - DiploFoundation)***
Certificate, e-Governance in Developing States ***(University of the West Indies)***
Certified Information Systems Security Professional ***(ISC)2***
Certified Information Systems Auditor ***(ISACA)***
Certified Data Privacy Solutions Engineer ***(ISACA)***

Roles Held:

Advisory/Virtual Chief Information Security Officer for 10+ organizations ***(Latin America & the Caribbean, Africa, Asia-Pacific, Middle East, and Europe)***
Chief Information Security Officer & Data Privacy Officer ***(United Nations Office for Project Services)***
Chief Information Security Officer & Data Protection Officer ***(Doodle)***
Chief Information Security Officer ***(Bemol)***
Team Leader / Key Expert, Cybersecurity & Digital Policy ***(European Commission)***
Director, Cyber-Policy Capacity Building ***(Internet Society)***
Senior Consultant, Privacy & Data Protection ***(Deloitte Consulting)***
Special Advisor on Cybercrime Prevention ***(Regional Security System)***
Chief Information Officer ***(Bermuda Commercial Bank)***
Chief Information Officer & Director, Integrated Information Systems ***(CARICOM Secretariat)***
Head of Network & Security Engineering ***(CIBC Caribbean)***
IT Risk & Legal Compliance Principal ***(Canonical)***

Presenter Bio - Niel Harper

Cybersecurity & Cybercrime || Digital Policy || Technology Management || Corporate Governance

Boards, Committees, & Working Groups:

Independent Management Advisory Committee ***(International Telecommunication Union)***
Professional Standards Working Group ***(UK Cyber Security Council)***
United Nations Information Security Special Interest Group ***(United Nations)***
Cyber Risk & Corporate Governance Working Group ***(World Economic Forum)***
Expert Networks for Cybersecurity, Data Policy, and Risk & Resilience ***(World Economic Forum)***
Chair, Innovation & Technology Committee ***(ISACA)***
Board of Directors ***(ISACA)***
Board of Directors ***(ISACA Foundation)***

Awards & Recognition

Top 25 Cyber Security Leaders for 2024 ***(Cyber Security Hub)***
Young Global Leader ***(World Economic Forum)***
Global Shaper ***(World Economic Forum)***
Technology for Humanity Award ***(ISACA)***
Caribbean Security & Resilience Award ***(Information Security Journal)***
Next Generation Leader ***(Internet Society)***
Alumni of Excellence Award - Technology ***(Algonquin College)***
Chartered Fellow ***(British Computer Society)***
Fellow, Cybersecurity Strategy & Leadership ***(CIFAL Miami)***
Fellow to the OECD Technology Foresight Forum ***(OECD)***
Fellow to the American Registry for Internet Numbers ***(ARIN)***
Fellow ***(Royal Society of Arts)***

Headlines - Abuse of Cybercrime Laws

How cybercrime laws are silencing dissent in Mideast

Between a hack and a hard place: how Pegasus spyware crushes civic space in Jordan

RESTRICTING FREEDOM OF EXPRESSION ONLINE IN THAILAND

Sri Lanka's controversial internet safety law comes into force

Supreme Court narrows scope of sweeping cybercrime law

Digital Rights in Thailand in 'Free Fall' Analysts Say

More accountability: U.S. blocklists Sandvine for enabling digital repression in Egypt

The Growing Threat of Cybercrime Law Abuse: LGBTQ+ Rights in MENA and the UN Cybercrime Draft Convention

Philippines: Rappler Verdict a Blow to Media Freedom

Social media restricted, mobile internet cut in Senegal amid political unrest

Censorship at the door: India must say no to government fact-checking

Türkiye: Big tech should protect free speech and resist state censorship

In Pakistan, threats continue to internet access, including social media

Digital rights watchdogs warn against internet shutdowns in Togo ahead of elections

Part II, 4 (1-2) - Illegal access

4. (1) A person who intentionally or recklessly and without authority,

(a) gains access to the whole or any part of a computer system;
(b) causes a programme to be executed;
(c) or uses a programme to gain access to any data,

(2) For the purposes of subsection (1), the form in which any programme or data is accessed or obtained and, in particular, whether or not it represents a form in which it is capable of being executed is immaterial.

COMMENTS:

This section is too broad in its scope and can implicate innocent or well-meaning individuals such as cybersecurity testers, researchers, activists, and whistle-blowers. It's even more problematic where judicial officers aren't trained to understand how to distinguish criminality from activities that serve the public interest, protect organizations, or advance the cybersecurity profession. Certain guidelines should be included with the legislation to distinguish between acceptable and criminal behaviours. This is common practice with legislation in the UK and EU (e.g., Preamble, Explanatory Report, etc.). For example, the Explanatory Report for the Budapest Convention covers the background, scope, objectives, and main provisions of the framework, as well as the challenges and opportunities of cybercrime.

*There are also **specialized courts** (e.g., King's Bench Division for Technology and Construction) and/or **specialist judges** (e.g., Masters) in jurisdictions to address specialist law areas such as cybercrime.*

Part II, 5 (1-3) - Modification of programme or data

5. (1) A person who intentionally or recklessly and without authority causes any modification to a programme or data is guilty of an offence and is liable on conviction on indictment to a fine of $70000 or to imprisonment for a term of 7 years or to both.

(2) For the purposes of subsection (1), the act in question need not be directed at

(a) any specifically identifiable programme or data or type of programme or data; or
(b) any programme or data that is held in a specifically identifiable computer system.

(3) For the purposes of subsection (1), it is immaterial whether the modification is or is intended to be permanent or temporary.

COMMENTS:

*This section is misaligned with the Budapest Convention, Commonwealth Model Law on Cybercrime, Malabo Convention, and other cybercrime model laws which don't mention **"modification of programmes or data"** in terms of criminality. It also uses outdated language and criminalises several modern, productive use cases for software and data processing (e.g., AI, free and open-source software, open data policies, Creative Commons, data mining, etc.).*

*This section should be removed and can be addressed by Part II, 6 - Interfering with programme or data (which should be changed to **'Interfering with data'** for better alignment with the Budapest Convention).*

Part II, 6 (1-3) - Interfering with programme or data

6. (1) A person who intentionally or recklessly and without authority

(a) copies or move a programme or data

(i) to any storage medium other than that in which that programme or data is held; or
(ii) to a different location in the storage medium in which that programme or data is held;

(b) destroys or erases a programme or data […]

(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.
(3) For the purposes of subsection (1), the form in which a programme or data is copied and, in particular, whether or not it represents a form in which it is capable of being executed is immaterial.

COMMENTS:

As with the previous section, Part II, 6 (1-3) also uses outdated language and criminalises several modern, productive use cases for software and data processing (e.g., AI, free and open-source software, open data policies, Creative Commons, data mining, etc.) The determinant for criminality should be, ***"A person who intentionally without authority and causes serious harm damages, deletes, deteriorates, suppresses, or alters computer data…"*** *If an act is temporary and causes no serious harm, it shouldn't necessarily be a crime. Part II, 6 (3) is unnecessary, adds little clarity or value, and can result in confusion, especially for untrained judges and magistrates.*

Part II, 7 - Interfering with computer system

7. A person who intentionally or recklessly and without authority,

(a) hinders the functioning of a computer system by

(i) causing electromagnetic interference to a computer system;
(ii) accessing or causing access to a computer system; or
(iii) corrupting a computer system by any means; or

(b) interferes with the functioning of a computer system,

COMMENTS:

This is poor legislative drafting which can potentially lead to criminalization and heavy-handed penalties for minor and/or accidental interference with computer systems. The drafting should focus on establishing a criminal offence where the actions are ***"intentional without authority to seriously hinder the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."***

Part II, 8 - Illegal interception of data

8. A person who intentionally and without authority, undertakes an act to intercept by technical means any non-public transmission to, from or within a computer system, including electromagnetic emissions from a computer system carrying computer data [...]

COMMENTS:

Poor legislative drafting and indicative of a lack of understanding of modern computer systems and data governance.

The criminal offence should be focused on ***"interception without authority of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions."*** *There should also be qualifiers that the intent is* ***dishonest*** *and/or* ***harmful****.*

Part II, 9 - Misuse of devices

9. A person who intentionally or recklessly and without authority,

(a) produces, sells, procures for use, imports, exports, distributes or otherwise makes available

(i) a device, including a computer programme, that is primarily designed or adapted for the purpose of committing an offence; or
(ii) computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent that it be used by any person for the purpose of committing an offence; or

(b) has an item mentioned in paragraph (a) (i) or (ii) in his possession with the intent that it be used by himself or any other person for the purpose of committing an offence,

COMMENTS:

There are several dual use programmes and applications which can be and are used for both legitimate testing and protection of computer systems and conversely for malicious intent. There should be language here which acknowledges such and removes criminality in cases of ethical hacking for instance. The Budapest Convention particularly states that the production, sale, procurement for use, import, distribution or otherwise making available or possession of a device in relation to offences in Part II, 4-9 ***"…shall not be interpreted as imposing criminal liability where [it] is not for the purpose of committing an offence […] such as for the authorised testing or protection of a computer system."***

Part II, 12 (1-4) - Critical information infrastructure system

12. For the purposes of this section “critical information infrastructure system” means any computer system, programme or data that supports or performs a function that relates to

(a) electricity generation or distribution;

(b) telecommunications;

(c) government services;

(d) emergency services […]

COMMENTS:

This section is unnecessary, the offences and penalties are already addressed in other sections, and critical infrastructure (CI) protection needs to be dealt with more comprehensively in ***separate legislation****. The CI protection legislation should effectively oblige a broad cross section of entities and sectors to take measures that would assist in increasing the level of cybersecurity in Barbados in the longer term. This section does precious little to protect CI as it* ***does not legally oblige public or private service providers to implement strong cybersecurity measures that would go much further in defending against malicious threat actors****.*

Part II, 19 (1-2) - Malicious communications

19. (1) A person who intentionally or recklessly uses a computer system to publish, broadcast or transmit computer data that

(a) intimidates a person; or

(b) threatens to

(i) use violence towards a person or a member of his family; or
(ii) damage the property of a person or the property of his family

COMMENTS:

The offences are legitimate but may be more aptly addressed in separate legislation that addresses criminal abuse, violence and harassment (e.g., Criminal Damage Act, Offences Against the Person Act, etc.). This includes revenge porn and online harassment.

Criminality around online threats should focus on intention, specificity, and credibility. The threat must be capable of placing someone in fear of harm and lead them to conclude that the threat is credible, real, and imminent.

Part II, 19 (3-5) - Malicious communications

19. (3) A person who intentionally uses a computer system to disseminate any image or words, not caring whether they are true or false, and causes or is likely to cause or subject a person to ridicule, contempt or embarrassment, is guilty of an offence [...]

COMMENTS:

The offences are legitimate in some cases but may be more aptly addressed in separate legislation that addresses criminal abuse, violence and harassment (e.g., Criminal Damage Act, Offences Against the Person Act, etc.). Additionally, criminality in terms of intimidation/threats should focus on ***intention****,* ***specificity****, and* ***credibility****. Threats must be capable of placing someone in fear of harm and lead them to conclude that the threat is credible, real, and imminent.*

Criminal defamation is outdated and widely seen by legal experts as susceptible to abuse and infringement upon freedom of expression. Debate on public issues should be uninhibited, robust, and wide-open, and may well include unpleasant attacks on individuals (including government and public officials). Defamatory statements can be treated in civil courts. ***The European Court of Human Rights, United Nations Human Rights Committee, several human rights organizations, and inter-governmental bodies maintain that criminal defamation laws are an unjustifiable affront to human rights****. Several progressive countries have removed criminal defamation from their books and are focusing only on civil defamation.*

The Budapest Convention and other cybercrime model laws do not address malicious communications in the context of cybercrime.

Part II, 20 (1) - Cyber bullying

19. (1) A person who intentionally uses a computer system

(a) to publish, broadcast or transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene or of a menacing character or causes any such data to be so sent;

(b) for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress to that person

COMMENTS:

Without safeguards/protections, vague laws around transmission of data that causes ***"annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress"*** *can be used to violate freedom of expression and suppress open public discourse.*

Cyber bullying 'laws' in the US, UK, Canada, Australia, and other countries mostly focus on preventing bullying in schools - children and adolescents. There are generally no specific cyberbullying laws in the previously mentioned countries, but existing laws for criminal abuse, violence and harassment are used to address cyber bullying as a crime. Adult cyber bullying is generally restricted to violent acts, sexual abuse, or harassment (adults are expected to be more resilient to hurtful words).

There should be guidelines developed to address cyberbullying cases. For example, the UK's Crown Prosecution Service, which oversees conducting criminal prosecutions in England and Wales, has guidelines for cases of cyberbullying.

Part III, 23 (1-6) - Search and seizure

23. (1) Where a Judge or magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for suspecting that an offence has been, is being or is about to be committed in any place and that there is evidence that such an offence has been, is being or is about to be committed in that place, the magistrate may issue a warrant authorising any police officer to enter and search that place, including any computer system, using such reasonable force as is necessary […]

COMMENTS:

This gives law enforcement excessively broad powers when it comes to confiscation and access to computer systems (including smaller form factors such as tablets and mobile phones). These types of powers require protections and safeguards to counteract abuse and misuse.

The Government of Barbados needs to be transparent with citizens about how their personal data which is processed in relation to the Cybercrime Bill is protected. This includes publishing general or public notices on the legal basis for processing, retention periods for the data, who the data is being shared with (e.g., international police organizations, foreign law enforcement, professionals / consultants working with law enforcement, etc.), and what redress is available to individuals with regards to misuse and abuse of their personal data. If someone is not guilty of a crime or is no longer being investigated in relation to a criminal matter, law enforcement has no legal basis for keeping their data and should delete it. If a legal basis remains, this needs to be formally explained in detail to the individual. This includes any data captured related to content from someone's computer, laptop, and mobile phone or their location data and Internet usage activities.

Part III, 24 (1-5) - Assisting a police officer

24. (1) A person who

(a) is in possession or control of a computer data storage medium or computer system; or

(b) has knowledge about the functioning of a computer system or measures applied to protect the computer data therein,

that is the subject of a search or a seizure, shall assist a police officer in the execution of a warrant issued under section 23 […]

COMMENTS:

Some of the provisions in this section are problematic and can be used to force individuals to grant access to their personal devices under duress or fear of imprisonment, especially if the grounds for disclosure have not been met.

This section appears to robs individuals of the privilege against self-incrimination and relieves law enforcement of the responsibility of having the capabilities of obtaining the evidence for prosecution themselves.

Again, this requires independent and effective oversight functions, and the oath of a police officer shouldn't be enough to obtain a warrant that grants such far reaching powers.

Part III, 26 (1-3) - Production of data for criminal proceedings

26. (1) Where a Judge or magistrate is satisfied on the basis of an application by a police officer that specified computer data or other information is required for the purpose of a criminal investigation or criminal proceedings, the Judge or magistrate may order that

a person shall submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; or […]

COMMENTS:

Common guidelines should be developed for both law enforcement and service providers and specific guidelines for each of them in terms of how subscriber data is requested and how those requests are fulfilled. This is not to substitute the legislation but instead to supplement and help the cybercrime legislative framework be effective in practice. Strong, documented prior judicial authorisation by a court or an independent judicial authority should be obtained to issue an order in all instances. As evidence will increasingly be stored in online services outside of Barbados, training and guidelines should also be developed for cooperation with law enforcement in other jurisdictions with respect to cross-border access to electronic evidence (e-evidence).

Should ensure that the Supreme Court publish, at a minimum, aggregate information on the specific number of requests approved and rejected, a disaggregation of the orders by service provider and by investigation authority, type, and purpose, and the specific number of individuals affected by each request.

Should impose a minimum factual basis necessary to access subscriber information only when the person investigated is suspected of planning, committing, or has planned or committed criminal acts.

Should exclude location data or any data that can reveal precise conclusions concerning the private lives and daily habits of a subscriber. Should require that law enforcement and/or service providers ensure that data disclosed pursuant to an order will not, cross-referenced with other data, result in an unexpected level of intrusion on individuals' private lives.

Part III, 28 (1-3) - Preservation of data for criminal proceedings

28. (1) The Commissioner of Police or any other gazetted officer may make an *ex parte* application for a preservation order to a Judge or magistrate where

(a) computer data, including traffic data, stored in a computer system is required for the purposes of a criminal investigation; and

(b) there are grounds to believe that the computer data, including traffic data, stored in a computer system is particularly vulnerable to loss or modification […]

COMMENTS:

*There is no discussion of the **conditions** and **safeguards** for adequate protection of human rights and liberties when collecting and storing (preservation) data for criminal proceedings.*

*This includes maintaining the **"chain of custody"**, protection of personal data in line with the Data Protection Act, handling of sensitive data, retention periods, adequate security measures, automated decisions (e.g., use of AI), cross-border transfers, sharing personal or sensitive data with third-parties, records of how data is accessed and used, etc.*

The provisions should also include guidelines for strong judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such powers or procedures.

Part III - General observations

Part III (Investigation and enforcement) is missing key provisions related to:

(a) Joint investigations or joint investigation teams

(b) Expert witness testimony by video conferencing

(c) Emergency mutual assistance (which is different to expedited disclosure)

(d) Procedures enhancing direct co-operation with entities and providers in other countries

(e) Procedures enhancing international co-operation between authorities for the disclosure of stored computer data

Cybercrime capacity building

Training of law enforcement officers, prosecutors, magistrates, and judges especially with regards to the below areas is a major problem in the country. Because these specialist areas of law are emerging, there is poor understanding of the issues by magistrates, judges, prosecutors, etc. and limited case law to refer to locally or in other regional jurisdictions. Consequently, many rulings / decisions have flawed bases, and individuals are often under- or over-penalised.

Adopt a multidisciplinary approach in the broader sense, to include:

(a) different disciplines within the law (including international comparative jurisprudence)

(b) different skills required to apply the law

c) e.g., science, technology, digital forensics, electronic evidence (e-evidence), privacy & data protection, financial frauds, intellectual property rights, child pornography, digital copyright, terrorism, human trafficking, online sexual exploitation, online drug trafficking, Dark web, cryptocurrencies, etc.

The Barbados Bankers Association Inc.
Goddards Complex, Fontabelle, St. Michael, Barbados
Telephone: (246) 430 6541
E-mail: tbba@tradeteam.bb

May 14, 2024

Parliament,
Parliament Buildings,
BRIDGETOWN
For the attention of Mr. Pedro Eastmond, Clerk of Parliament

Dear Sir,

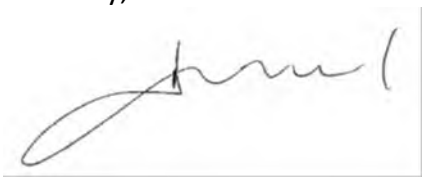
Re: Cybercrime Bill, 2024

The Barbados Bankers Association ("**TBBA**") refers to your correspondence on the captioned subject.

Attached please find comments submitted on behalf of the TBBA.

We thank you for the opportunity to be part of the process.

Sincerely,



Anthony Clerk
PRESIDENT

Enc.

The Barbados Bankers Association Inc.
Goddards Complex, Fontabelle, St. Michael, Barbados
Telephone: (246) 430 6541
E-mail: tbba@tradeteam.bb

Cybercrime Bill, 2024-A REVIEW

Purpose: An Act to provide for the combatting of cybercrime, protection of legitimate interests in the use and development of information technologies, the facilitation of international co-operation in computer related crimes and related matters.

Part II Section	Comment
13(2)	**Receiving or giving of access to computer programme or data** This section creates a defense to a charge brought under subsection 13(1) where the programme or data or access to the programme or data (a) was received inadvertently and with no intent to commit an offence; (b) was subject to legal privilege; **and** (c) was received by a law enforcement officer in the course of an investigation. The emboldened "**and**" should be replaced by "**or**"
16(1)	**Child pornography** This section penalizes a person who intentionally or recklessly publishes…produces…possesses…procures child pornography.

Part II Section	Comment
	Greater protection should be afforded to publishers whose platforms are used for such purposes despite prohibitions against the same, provided that the publishers are not negligent in removing the offending material.
19	**Transmitting data which causes substantial emotional distress** A person who intentionally or recklessly uses a computer system to publish, broadcast or transmit computer data that intimidates a person is guilty of an offence. "Intimidate" includes causing substantial emotional distress. The wide nature of this provision would seemingly endanger a Bank's ability to transmit correspondence to a customer that advises him that enforcement action may follow if a facility is not repaid by a certain deadline.
20	**Cyberbullying** A person who intentionally uses a computer system for the purpose of causing embarrassment, humiliation, anxiety or causes substantial emotional distress to that person is guilty of an offence. Like section 19, this clause also seems to be unduly wide and could impact a Bank's communication of negative news to its customer.
22	**Aiding and Abetting** This section penalizes a person who aids or abets the commission of an offence under the Act There should be clear protection for employers whose employee or contractor uses his work email address or bank issued device, to distribute/commit an offence that is outside of his duties.
Part III Section	**Comment**
23	**Search and seizure**

Part II Section	Comment
	Section 23(2)(d) authorizes a police officer to "have access to any information, code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer system into readable." Where providing such code would endanger the security of other data which is not relevant to the offence, an option for the data to be decrypted for the officer should be an option. This section should include protection for "privileged information or material" as is done under the Proceeds and Instrumentalities of Crime Act.
26(2)	**Production of data for criminal proceedings** This section provides that "a person referred to in subsection (1) who discloses without authority any information in his possession or under his control is guilty of an offence and is liable on conviction on indictment." This section is wide and prevents any disclosure of any information. It may instead have been intended to prevent tipping-off and should be reworded.
General	**Comment**
	Scope of "without authority" Several provisions create offences where actions are taken "without authority". It is recommended that there be a definition which confirms the scope of those words to ensure that persons acting in accordance with consent, a legal or contractual basis, on the basis of professional advice or in good faith are protected.
	General Defenses Several sections provide defenses but others do not. For instance, the defenses at section 19(5) are only available to offenses under section 19(3) but not sections 19(1) and (2). It is recommended that there should be general defenses available, particularly that at section 19(5), ie the defences of truth, comment, triviality and privilege, whether absolute or qualified, provided for under the Defamation Act, Cap. 199.

The Barbados Bar Association
Report to Joint Select Committee of Parliament
on
Cybercrime Bill, 2024

Executive Summary

The Barbados Bar Association (BBA) recognises the importance of establishing a statutory regime provide rules of conduct and acceptable modes and standards of behaviour for the use of the Internet, computers, and related digital technologies, both now and in the future. It is also noted that the UNODC United Nations Office on Drugs and Crime Cyber states that crime legislation enables the investigation and prosecution of crimes committed online and facilitates cooperation between countries on cybercrime matters (UNODC, 2013, p. 52)

It is equally important however to balance this and protect the fundamental rights and freedoms of the citizens of Barbados, freedoms such as freedom of speech and expression as enshrined in the Constitution of Barbados. The public of Barbados are entitled to expect responsible and proper exercise of public power, which is fundamental to the operation of the rule of law.

Through its Law Reform and Legislation Committee, The Barbados Bar Association sought feedback from its members and conducted a comparative review of regional and international legislation. The Committee ended its report as follows:

> *'The Committee concludes that the level of debate and interrogation of this Bill to date has been inadequate given the very serious power which is being vested in the State and in private individuals in matters protected by the Constitution, that is to say, the rights to privacy and expression.*
>
> *Unless amended the Bill will inevitably face challenge in the Courts.'*

The BBA:

1. cautions the framers to consider the language of the Bill, in particular where may have the effect of importing legal terms which heretofore do not exist in this country's legislative framework;
2. recommends a careful examination of powers proposed to be conferred, the rules of evidence and criminal procedure, and other criminal justice matters in the Bill;
3. re-examine the unintended consequence of the proposed repeal of section 34 of the Defamation Act Cap. 199

This document treats to various sections of the Bill, and reflects and incorporates member feedback thereon. The Barbados Bar Association will seek to expand on its comments in its oral presentation, through the Clerk of Parliament, before the Joint Select Committee of Parliament and is appreciative of the invitation to participate in the crafting of what is a seminal piece of legislation.

Barbados Bar Association
14th May 2024

The Law Reform Committee
The Barbados Bar Association
Leeton Gap, Bridgetown

Report on the Cybercrime Bill, 2024

1 The Law Reform Committee has reviewed the above caption Bill and now presents its report.

2 The Cybercrime Bill, 2024 is the same one which was circulated through the Barbados Bar Association in March 2022.

3 The explanatory memorandum, which accompanied the Bill at that time, explained that the drafters received the assistance of the European Commission and the Council of Europe in modernising the framework for criminal accountability of the misuse of computer systems and programmes, having judged that the Computer Misuse Act, 2005 was no longer fit for purpose.

4 The draft Bill is based on the only enforceable multinational treaty on cybercrime, referred to in its shortened form as the Budapest Convention or Convention 185, which came into force on 1st July, 2004, with 5 ratifications back then.

5 As at 3rd March, 2024 both Grenada (requested 8th February, 2023 with an expiration in 2029) and Trinidad and Tobago (requested to accede on 15th July, 2021 with expiration in 2026) have asked to join in the application of the Treaty. Non-Council members have 5 years from the date to sign and accede, to ratify or to accede to the respective Treaties.

6 Trinidad and Tobago has attempted to pass similar cybercrime legislation in 2015 and 2017, both modelled on the Budapest Convention, and both failed to pass. Newspaper articles, as at 2023, indicate that TT is working on a redraft.

7 (i) It is to be noted that there was no consensus on the UN Treaty on Cybercrime, for which negotiations started in January, 2022 and ended in February, 2024. This was an initiative of Russia (letter dated 11/10/2017, Agenda item 107 on Crime Prevention and Criminal Justice, 72nd session, Third Committee UN General Assembly). The main criticisms from NGOs were that governments were seeking expansive powers, amounting to surveillance on its citizens, rather than targeted use, without balancing those with human rights and/or procedural safeguards, which could result in criminalising ordinary internet activities.

(i) There was also no consensus as to the meaning of cybercrime under the UN Treaty, with a few countries pushing for content related crimes such as disinformation and, of course, copyright infringement. Some countries suggested that the seriousness of the cybercrime be determined by the severity of the penalty rather than by the elements of the crime and one could reasonably ask whether any of this type of analysis filtered into the penalties and wording of a few sections in the Cybercrime Act, 2024 (see paragraph on section 9, for instance).

8 Unlike the Computer Misuse Act, 2005-4, the aim of which was simply to protect computer systems and the information contained therein from unauthorised access and abuse, the Cybercrime Act, 2024 appears to go much further, with a stated aim being for 'the protection of legitimate interests in the use and development of information technologies…' This suggests the proposed use of surveillance/profiling, and/or the use of traffic data and perhaps meta data: and it also suggests, perhaps without the public's knowledge, content on a wider scale than anticipated (these will most definitely engage the provisions of the Data Protection Act, 2019 and the Constitution).

9 The scope of offences covered by the Cybercrime Act, 2024 extends to illegal access of computer systems, unauthorized, intentional or reckless modification of a programme or data, unauthorized, intentional or reckless interference with a programme or data or computer system intentionally, recklessly and without authority receiving or giving access to computer programmes or data (s 13); illegal interception of data by a person (S.8), misuse of devices (section 9 is open-ended), access with intent to commit further offences, disclosure of codes, interfering with critical infrastructure systems as defined with the Act (s 12), committing computer related forgery as defined within the Act (s 14), committing computer related fraud as defined within the Act (s 15), child-related offences of online child sexual abuse (s 18), child pornography (s 16), child grooming (s 17), cyber bullying applicable also for the protection of adults (s 20) (perhaps there have been amendments in the Sexual Offences Act), cyber terrorism (s 21), aiding and abetting (s 22).

10 The Committee did not see any criminal offence relating to identity theft in the Cybercrime Act: the focus is more on protecting assets. Section 24 of the Barbados Identity Management Act, 2021 somewhat alludes to identity theft, carrying a very low term of 6 months imprisonment and limited to offences under the Act.

11 The Cybercrime Act, 2024 does not contain any cross reference to the new Child Protection Act, 2023 which, under section 2, provides definitions of 'cyber-abuse' and 'sexual abuse' (includes grooming and sexting or cyber-abuse).

Cyber terrorism

12 (i) The law and amendments surrounding the Constitution as well as the Anti-Terrorism Act are rather confusing since government websites do not present the law in a consolidated form. It appears that the Anti-Terrorism Act, Cap 158 was renamed the Anti-Terrorism and Counter-Proliferation of Weapons of Mass Destruction Act by virtue of section 3 of the Anti-Terrorism (Amendment) Act, 2019-34.

(ii) If the above is correct, the name 'Anti-Terrorism Act' in section 21(2) of the Cybercrime Act, 2024 appears to be a misnomer, and the term of imprisonment in that section should be cross-checked with the amendments made by the Anti-Terrorism (Amendment)Act, 2019-34 to the principal Act, Cap 158.

(iii) Cyber terrorism does not appear to be capable of being committed by an entity under section 21 of the Cybercrime Act, 2024. However, section 5 of Cap 158 seeks to ensure that conviction on indictment to a fine of $2 million can be imposed on a legal entity where terrorism or its financing is committed by 'a person responsible for the management or control' of the entity. 'Control' of a company could be synonymous with a 'majority shareholding' in that company, and it is not clear whether it was the intention of the drafters to impose liability on shareholders; further, 'management' is not specified as precisely as under section 43 of the Anti- Corruption and Anti-Terrorism Agency Act, 2021-5: under the latter Act, a director, manager, secretary or other officer as well as the company itself could be held criminally liable for hindering corruption or terrorism investigations by officers of the Agency. The specified persons could face imprisonment or fines.

Offences relating to children

13 (i) Child pornography, grooming and on-line child sexual abuse are the three offences under the Cybercrime Act, 2024 which impose criminal fines on a corporation. Of these three, only section 16, the child pornography section, clearly has the *actus reus* in (c) and the *mens rea*, intentionally or recklessly, which are capable of attaching to a corporation.

14 Oddly, section 17, the child grooming section, provides a criminal penalty for a corporation, though such *actus reus* is by its very nature inapplicable to a company (unless in cases of AI), namely befriending, etc, a child in order to carry out abuse. It would be a different matter if the *actus reus* were expressed as, for instance, 'or facilitating the use of a computer system' in order to abuse a child. In such a case, a corporation (device makers) and even a service provider would be obliged under the law to conduct device scanning (Application section 3).

(i) The same analysis as applied to section 17 applies to section 18, the online child sexual abuse regarding corporations. Sexual activity is not defined under the Cybercrime Act, 2024 nor under the proposed Child Protection Act, 2023. However, sections 21(2) and (3) of the Interpretation Act allow for officers of corporate entities to be charged and prosecuted as if they had committed offences in their personal capacities. Such prosecutions may only be initiated with the permission of the Director of Public Prosecutions.

(ii) Section 24(1) (g) of the Child Protection Act, 2023 provides for mandatory reporting for an internet provider…..or telecommunications technician who has knowledge or has reasonable grounds to suspect that a child is in need of care and protection within the meaning of section 5 of that Act. Abuse under section 2 of that Act includes cyber-abuse as defined to include cyber-bullying, cyber-harrassment and exposure to harmful images by electronic means.

(iii) The questions the public need to have answered are:

(a) How would a corporation such as an internet provider or a telecommunications technician inside a telecoms company know, for instance, that a child was being groomed, unless the law now required them to have access to or monitor the meta data/content of communication or traffic and on private over the top encrypted communications (WhatsApp) in a much different manner?

(b) Given aim (b) of the Objects and Reasons of the Cybercrime Act, what are the legal safeguarding measures put in place to respect the privacy of residents from systematic surveillance and abuse of authority by any cybercrime agency/unit yet to be established (gazetted officer)?

15 There is a need for examination by legal specialists as to whether there are sufficient human rights and/or judicial and procedural safeguards for individuals accused of crimes under the Act (other than those under the Constitution and the Data Protection Act, 2019-24).

Dual criminality not a bar in preservation of computer data

16 (i) We also note that, under section 20A(3), dual criminality shall not be a requirement in complying with a request for assistance in expediting preservation of computer data for a Commonwealth country under the Mutual Assistance in Criminal Matters (Amendment) Act, 2024. Of the 56 member states of the Commonwealth, there are at least three which have arguably suspect human rights records. [Please check whether this section is Constitutional.] The Mutual Assistance in Criminal Matters Act, Cap 140A

(s 29) covers non-Commonwealth countries through bilateral treaty with Barbados (amendment made by the Anti-Terrorism Amendment Act, 2015-28 and a country which is a party to the Budapest Convention on Cybercrime (by the proposed amendment section 5 of the Mutual Assistance in Criminal Matters (Amendment) Act, 2024).

(ii) What if the definition of a particular crime (such as terrorism) under local legislation does not match the definition of a particular crime in another country or under an international treaty for the reason that there is no universally acceptable definition of it? Is that a necessary or proportionate justification upon which a police officer could obtain a search and seizure warrant? This has been a reason why activist groups have criticised the inclusion of cyber terrorism in the UN Treaty on Countering the Use of Information and Communications Technologies for Criminal Purposes.

Misuse of Devices -open ended 'committing an offence'

17 (i) The substantive scope of section 9 on the Misuse of Devices seems not to be limited to offences as specified in the Act. The scope of offences is open-ended and is perhaps meant to sweep in breaches under the new Copyright Act 2023 (referenced in the Schedule as a Consequential Amendment) (tabled in Parliament), Parts X and XI, concerning the use of devices designed or adapted to circumvent copyright protection or to alter rights management information from copies of copyright work and any other offence which may fall within the proposed new section 20A(3) amendment to the Mutual Assistance in Criminal Matters Act, Cap 140A on dual criminality or even any other offence created in the future.

(ii) It seems that, under the Cybercrime Act, the severity of offences is measured by the length of terms of imprisonment rather than the elements of the offences. The penalty for 'an offence', which could mean for 'any offence' is 7 years, whereas under the Computer Misuse Act (which limits the offences to sections 4,5,6 of that Act) carries a term of imprisonment of 5 years. It is noteworthy that 12 times under the Cybercrime Act, 2024, a term of imprisonment carries a 7-year penalty. A 7-year term of penalty under the Computer Misuse Act is mentioned just twice; 5-year terms are included in the latter Act 10 times.

Please note that the Computer Misue Act, section 8, limits offences to those committed within certain sections of the Act. Article 6 of the Budapest Convention itself also limits offences within Articles 2 to 5.

Malicious communications

18 The offences in sections 19(1) and (2) of the Cybercrime Act, as drafted, certainly can also be committed by a corporation but there are no penalties attached to them. A reasonable speculation as to why this is so could be that this will lead to systematic monitoring by a service-provider or produce more onerous effects on private companies to police their networks for written content.

19 Section 19 (3) which appears to be the most spoken about by members of the public and a few members of the Bar. It is the section which appears to mirror a civil right of action for defamation with criminal defamation whilst allowing specified defences under the Defamation Act, Cap 199. One of those crucial defences maintained under the Cybercrimes Act is the *Reynolds* public interest defence.

20 It is known that the Council of Europe is promoting the abolition of criminal defamation as not only repressive regimes abusing its use to limit freedom of expression but also western, democratic governments are doing the same against journalist bloggers, investigative journalists, campaigners/advocates, whistleblowers, comedians and satirists, artists who have the important role of participating in public affairs as public watchdogs, encouraging the accountability and transparency of those who hold public office, or of those who are public figures. A 2023 report update, 'SLAPPS: A Threat to Democracy Continues to Grow', by the Coalition Against SLAPPS Europe (CASE), has indicated that there were over 570 private censorship cases across Europe over a ten-year period. (Unknown whether it is possible to conduct the same type of legal analysis in the Caribbean).

21 There is also a draft EU Directive on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings Com (2022) 177 Final, awaiting formal adoption.

22 The UK abolished the common law of criminal defamatory libel in 2010 through section 73 of the Coroners and Justice Act, 2009, in recognition that it has been used by other countries to curtail that freedom of expression which is absolutely necessary for the functioning of a free and democratic State.

23 (i) Based on public comments circulating in Barbados, there appears to be a public perception that section 19(3) may be used by public figures to curtail freedom of expression. Just in October, 2023, Barbados brought into force the Prevention of Corruption Act, 2021-24 which by section 21 incorporated the United Nations Convention Against Corruption (adopted in 2003). Thus, section 19(3) appears to be incongruent with the legislation recently brought into force.

(ii) Article 13 of that Convention requires States to bring into domestic law the 'active participation of individuals and groups outside the public section… in the prevention of and the fight against corruption and to raise awareness of the threat..'. One such initiative is demonstrated in Article 13 1 (d)….

Respecting, promoting and protecting the freedom to seek, receive, publish and disseminate information concerning corruption with curtailment on the ground of necessity (i) for the respect of the rights or reputations of others; (ii) the protection of national security or public order or public health or morals.

24 Section 19 (3) of the proposed Cyber Crimes Act 2024 contains the following language: *"A person who intentionally uses a computer system to disseminate any image or words, not caring whether they are true or false, and causes or is likely to cause or subject a person to ridicule, contempt or embarrassment, is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both."*

25 Further, when the Act becomes law, it may have the effect of impliedly amending several other statutes. One such amendment would affect the law of criminal libel as established by s.34 of the Defamation Act. S. 34 to the following effect:

"(1) Liability for criminal libel shall extend to charges contained in matter published (a) by means of broadcasting; or (b) in permanent form.

(2) The defence of comment and the defence of privilege (whether absolute or qualified) shall extend to a prosecution for criminal libel as they respectively extend to an action for defamation.

(3) A court of summary jurisdiction shall, with the consent of the defendant, have power to hear and determine a prosecution for criminal libel and shall have power to impose on conviction a fine not exceeding $2 000 or imprisonment for a term not exceeding 12 months or both.

(4) No prosecution for criminal libel shall, without the consent of the Director of Public Prosecutions being first obtained, be brought in respect of any matter appearing in a newspaper or periodical publication against any proprietor, publisher, editor or other person responsible for the publication of such newspaper or periodical publication or against any person who (whether or not employed by such proprietor) is paid to contribute matter to such newspaper or periodical publication; nor shall any prosecution for criminal libel be brought without such order in respect of any matter broadcast against the broadcasting authority concerned or against any person who (whether or not employed by such authority) is paid to present or contribute such matter."

26 Criminal libel is not defined in the Defamation Act and so the common law definition of the offence is implicated.

27 Criminal libel at common law was a misdemeanor triable only on indictment. A complainant would have to prove that the Defendant had published a libel that would expose him to 'ridicule, hatred or contempt."

28 It is apparent that s.19(3) of the Bill is intended to extend liability for criminal libel as established statutorily by s.34 of the Defamation Act.

29 However, the operative language of the proposed s.19(3) differs from the common law definition. The word "embarrassment' is employed rather than 'hatred'. This is an important departure as the law of defamation and criminal libel are recognized as permissible fetters on the constitutional right to freedom of expression, see section 20(2)(b) of the Constitution.

30 This raises the issue as to whether as currently drafted, s19(3) runs up against the constitutional right to freedom of expression. The question is whether a law which imposes a restriction on language which causes "embarrassment", is "reasonably required" in the interest of protecting the reputation of other persons and thereby rendered lawful by s.20(2)(b) of the Constitution.

31 The word "embarrassment" is not defined in the Bill. The usual canons of statutory interpretation dictate that the word 'embarrassment' must be given its usual and natural meaning in the context of which it is used. Embarrassment is defined in the Oxford online dictionary as a feeling of "self-consciousness, shame, or awkwardness". The use of this word seeks to introduce into the equation the reaction of a complainant to something published about him or her, rather than the reaction of those to whom the matter is published.

32 The gravamen of the offence of criminal libel is that the society in general will visit ridicule, contempt or hatred on the innocent party; How the target of the publication feels about what has been published is not relevant to establishing the actus reus of the offence. Injury to feelings may indeed, however, be relevant in determining the severity of the sanction imposed on a defendant where he is found guilty of criminal libel.

33 Insofar as s.19(3) of the Bill contains the word "embarrassment" it constitutes an unlawful contravention of the right to freedom of expression as guaranteed by s.20 of the Constitution and is liable to be struck down because it goes further than necessary in the protection of a person's reputation but would restrict the dissemination of information which may cause personal disquiet without more.

34 A Constitutional court would have the authority pursuant to the doctrine of severance to strike down s.19(3) only so far as it contains the word "embarrassment", leaving the rest of the section intact.

Does s.19(3) comply with the protection of the law guaranteed by s. 18 of the Constitution?

35 Criminal libel at common law was a misdemeanor triable only on indictment before a Judge and jury.

36 S.34(3) of the Defamation Act allows for a Magistrates Court to try a case of criminal libel if the Defendant consents. The penalty which can be imposed by a Magistrate is a fine of $2,000.00 or a term of imprisonment not exceeding 12 months or both.

37 S.19(3) of the Bill gives the Magistrates Court exclusive jurisdiction to hear and determine a charge brought thereunder and to impose a fine of $70,000.00 or to impose a sentence of imprisonment of 7 years or both.

38 S.18 of the Constitution demands that all persons charged with a criminal offence receive a fair trial within a reasonable time before an ***independent*** and impartial court.

39 Barbados law has recognized the role of the Magistrates Court in disposing of minor criminal offences. This is reflected in the short sentences which are generally visited upon persons upon summary conviction. The maximum sentence which a Magistrate may impose is usually 2 years. The only statute which grants a Magistrate the jurisdiction to imprison a person for more than 3 years is the Drug Abuse (Prevention and Control) Act 1990. This statue allows a Magistrate to impose a sentence of 7 years for certain serious drug offences.

40 The question of constitutional import is this. Is a Magistrates Court ***an independent court*** for the purposes of dealing with serious criminal matters with the power to impose long prison sentences on persons convicted by that court?

41 This very issue was canvassed in two cases before the Privy Council. Hinds et al v R (Jamaica) and Commissioner of Police v Davis (the Bahamas).

42 In **Hinds** the Privy Council set its face against Parliament transferring to officers of an inferior court the powers of punishment which had been the preserve of Judges of the Supreme Court. The impugned legislation, the Gun Court Act 1974, purported to empower a panel of 3 Magistrates in the Full Court Division the same power of sentencing as a Judge of the Supreme Court. The Law Lords held that in serious criminal matters the Constitution of Jamaica, guaranteed that an independent judiciary which enjoyed insulation from direct political pressure and/or interference was the institution which ensured fairness in the resolution of such matters. The provisions of the Gun Court Act 1974 which granted the Full Court Division such wide powers were struck down as unconstitutional.

43 Lord Diplock opined as follows:

"Where, under a constitution on the Westminster model, a law is made by the Parliament which purports to confer jurisdiction upon a court described by a new name, the question whether the law conflicts with the provisions of the constitution dealing with the exercise of the judicial power does not depend upon the label (in the instant case "The Gun Court") which the Parliament attaches to the judges when exercising the jurisdiction conferred upon them by the law whose constitutionality is impugned. It is the substance of the law that must be regarded, not the form. What is the nature of the jurisdiction to be exercised by the judges who are to compose the court to which the new label is attached? Does the method of their appointment and the security of their tenure conform to the requirements of the constitution applicable to judges who, at the time the constitution came into force, exercised jurisdiction of that nature?: Attorney-General for Australia v. The Queen [1957] A.C. 288, 309-310."

44 Lord Diplock later in this opinion states as follows:

"The attack upon the constitutionality of the Full Court Division of the Gun Court may be based upon two grounds. The first is that the Gun Court Act 1974 purports to confer upon a court consisting of persons qualified and appointed as resident magistrates a jurisdiction which under the provisions of Chapter VII of the Constitution is exercisable only by a person qualified and appointed as a judge of the Supreme Court."

45 Lord Diplock continues:

"If, as contended by the Attorney-General, the words italicised above in section 97 (1) entitled Parliament by an ordinary law to strip the Supreme Court of all jurisdiction in civil and criminal cases other than that expressly conferred upon it by section 25 and section 44, what would be left would be a court of such limited jurisdiction that the label "Supreme Court" would be a false description. So too if all its jurisdiction (with those two exceptions) were exercisable concurrently by other courts composed of members of the lower judiciary. But more important, for this is the substance of the matter, the individual citizen could be deprived of the safeguard, which the makers of the Constitution regarded as necessary, of having important questions affecting his civil or criminal responsibilities determined by a court, however named, composed of judges whose independence from all local pressure by Parliament or by the executive was guaranteed by a security of tenure more absolute than that provided by the Constitution for judges of inferior courts.

Their Lordships therefore are unable to accept that the words in section 97 (1), upon which the Attorney-General relies, entitle Parliament by an ordinary law to vest in a new court composed of members of the lower judiciary a jurisdiction that forms a significant part of the unlimited civil, criminal or supervisory jurisdiction that is characteristic of a "Supreme Court" and was exercised by the Supreme Court of Jamaica at the time when the Constitution came into force, at any rate where such vesting is accompanied by ancillary provisions, such as those contained in section 6 (1) of the Gun Court Act 1974, which would have the consequence that all cases falling within the jurisdiction of the new court would in practice be heard and determined by it instead of by a court composed of judges of the Supreme Court.

As with so many questions arising under constitutions on the West-minster model, the question whether the jurisdiction vested in the new court is wide enough to constitute so significant a part of the jurisdiction that is characteristic of a Supreme Court as to fall within the constitutional prohibition is one of degree. The instant case is concerned only with criminal jurisdiction. It is not incompatible with the criminal jurisdiction of a "Supreme Court," as this expression would have been understood by the makers of the Constitution in 1962, that jurisdiction to try summarily specific minor offences which attracted only minor penalties should be

conferred upon inferior criminal courts to the exclusion of the criminal as distinct from the supervisory jurisdiction of a Supreme Court. Nor is it incompatible that a jurisdiction concurrent with that of a Supreme Court should be conferred upon inferior criminal courts to try a wide variety of offences if in the particular case the circumstances in which the offence was committed makes it one that does not call for a severer punishment than the maximum that the inferior court is empowered to inflict. In this class of offences the answer to the question whether the concurrent jurisdiction conferred upon the inferior court is appropriate only to a "Supreme Court" depends upon the maximum punishment that the inferior court is empowered to inflict.

At the time of the coming into force of the Constitution the maximum sentence that a resident magistrate was empowered to inflict for any of the numerous offences which he had jurisdiction to try was one year's imprisonment and a fine of 100 dollars. It is not necessary for the purposes of the instant appeals to consider to what extent this maximum might be raised, either generally or in respect of particular offences, without trespassing upon the jurisdiction reserved by the Constitution to judges of the Supreme Court. The limit has in fact been raised to two years in respect of some offences including those under section 20 of the Firearms Act 1967. Their Lordships would not hold this to be unconstitutional; but to remove all limits in respect of all criminal offences, however serious, other than murder and treason, would in their Lordships' view destroy the protection for the individual citizen of Jamaica intended to be preserved to him by the establishment of a Supreme Court composed of judges whose independence from political pressure by the Parliament or the executive was more firmly guaranteed than that of the inferior judiciary.

It is this that, in respect of a particular category of offenders, is sought to be achieved by the provisions of the Gun Court Act 1974, relating to the jurisdiction and powers of a Full Court Division of the Gun Court."

46 In **Davis** the Privy Council were asked to strike down the provisions of the Dangerous Drugs Act which allowed for Magistrates to impose sentences of up to 5 years in prison.

47 Lord Goff of Chieveley stated as follows:

"Their Lordships would go further. As they read the judgment of Lord Diplock in Hinds v R [1976] 1 All ER 353 at 367, [1977] AC 195 at 219at 222, it is to the effect that, where the jurisdiction over the offences in question is exclusively vested in an inferior court, the question whether the jurisdiction so vested is appropriate only to a Supreme Court depends both on the nature of the offence and on the severity of the punishment which can be imposed; whereas where a concurrent jurisdiction is vested in the inferior court, the question depends upon the maximum punishment. ***It follows that, on the hypothesis that there was no entrenched right to trial by jury***

in the Constitution of the Bahamas, and that the relevant jurisdiction had then been transferred from the Supreme Court to the magistrates' courts, the question under consideration would be whether the offences could be characterised as minor offences and whether the punishment capable of being imposed could be characterised as a minor penalty. *(Emphasis added) If, however, the jurisdiction so transferred was concurrent with the jurisdiction of the Supreme Court, the question would relate only to the maximum punishment which the inferior court was empowered to inflict. On this approach, their Lordships have no doubt that a maximum sentence of imprisonment for life would inevitably render such transfer of jurisdiction unconstitutional on the principle in Hinds v R. In such a case, the transfer of the jurisdiction would be unconstitutional per se, though an additional effect would be that, since under the Bahamian Constitution it is a characteristic of offences charged on information in the Supreme Court that the accused is entitled to be tried by jury, by vesting in the magistrates' courts a jurisdiction to try offences which, under the Constitution, are properly triable only in the Supreme Court, the accused would inevitably be deprived of his constitutional right to jury trial".*

48 The High Court and the Court of Appeal of the Bahamas had held that a Magisterial jurisdiction to sentence persons convicted of drug offences to a maximum of 5 years in prison was within the threshold of constitutionality in the Bahamas, at least in part because drug offences had historically been treated more severely even at the Magistrates Court level, than other offences. The Privy Council also accepted that the Supreme Court had never had exclusive jurisdiction over drug offences in the Bahamas. The Privy Council elected not to depart from the opinions of the Bahamian Courts on this issue.

49 Criminal libel at common law can only be tried on indictment. The clear implication in s.34 of the Defamation Act which altered the common law, is that an allegation of criminal libel must be tried on indictment unless the Defendant consents to a summary trial in the Magistrates Court.

50 The offence created by s.19(3) of the Bill is an arrestable offence as defined by the Criminal Law (Arrestable Offences) Act Cap 125A as a conviction pursuant to s.19(3) is punishable by a term of imprisonment of more than 5 years. This offence is not a minor offence as defined by the Minor Offences Act Cap 137. (The maximum penalty under the Minor Offences Act is 3 years for a repeat offender.)

51 Given the foregoing, it is submitted on the authority of Hinds v R, that until Magistrates in Barbados are given the same constitutional protections as judges of the Supreme Court, Magistrates Courts cannot be considered as independent courts for the purposes of s.18 of the Constitution when dealing with serious criminal matters attracting prison sentences of up to 7 years.

52 In its current form s.19(3) is open to Constitutional challenge.

53 It is worthy of note that other offences in the Bill carry a 7-year sentence but are triable only on indictment. Given that s.19 is the only section which deals with the issue as to what information constitutes permissible lawful dissemination of ideas given the right to freedom of expression guaranteed by the Constitution, it is curious that such weighty legal matters would be entrusted to the Magistrates Court.

54 It is also to be noted that Magistrates Courts do not have the jurisdiction to hear allegations of defamation and that under the Juries Act, defamation is one of the few torts which gives rise to the right to a jury trial at the request of a party.

55 S.19(3) of the Bill is open to challenge constitutionally **BECAUSE**:

(i) The use of the word "embarrassment" introduces the subject element of the interpretation of statements by a complainant which causes a subjective 'feeling' in that person; Hurt feelings without reputational damage are not protected by the Constitutional insulation of laws designed to protect persons' reputations; and

(ii) The penalty of 7 years imprisonment may only be imposed by an ***independent*** court which for the purposes of the Constitution can only mean the High Court Division of the Supreme Court of Barbados because Judges of the Supreme Court enjoy Constitutional protection of their tenure in office, whereas Magistrates do not.

Additional Concerns

56 Section 13(2) of the Cybercrime Act, 2024 creates just three defences to receiving or giving unauthorised access to computer programme/data, none of which gives the press nor their sources any particular defence where receiving data is in the public interest. Neither does the Whistleblower Protections Act, 2021-29 create any opportunity for the press to be protected if they receive computer data they should not have received yet such data are in the public interest. In view of the fact that we currently do not have an explicit section protecting the press in the Constitution, in the interests of freedom of expression, the press should be given a special defence under section 13(2)..

57 Civil remedies for the law of defamation and breach of confidence and data protection may be sufficient and proportionate in providing protection for the rights of others or their reputations without recourse to the criminal law. However, in the same western democracies, it has been found that public figures often go beyond seeking rights to access justice to one of abusing their increased financial dominance and power in society to silence any form of criticism of them from as wide as for *issues* relating to corruption in public office to as far as obtaining super injunctions to prevent the disclosure of extra marital affairs. These very civil remedies have been used by SLAPPers throughout Europe, with the largest being grounded within the law of defamation. Anti-SLAPP laws have apparently existed in the USA since the 1990s

and, as at 7th September, 2023, 33 States have signed such legislation into effect. In Australia there is the Public Participation Act 2008, in Ontario, Canada the Protection of Public Participation Act, 2011, in British Columbia - the Protection of Public Participation Act, 2019 and a prior Act also in Quebec.

58 Many judicial systems including the Inter-American Court are beginning to reference the use of improper use of the court system to stifle freedom of expression.

59 In October, 2023 the UK enacted the Economic Crime and Corporate Transparency Act, 2023 Chapter 56. The anti-SLAPP provision, section 195 is limited in the interest of combatting economic crimes as defined within section 193 of that Act. Section 194 contemplates an amendment to the Civil Procedure Rules to facilitate the early disposal of SLAPP claims.

Unintended consequence of the repeal of s.34 of the Defamation Act

60. The Bill would effectively repeal the statutory offence of criminal libel which can be committed by way of broadcasting or publishing the libel in permanent form and replace it with an offence which can only be committed statutorily by a person using a computer system to disseminate the libelous material. It would mean that a person who is libeled by a radio broadcast which is not produced by a computer system as defined in the Bill, would have to bring a case for criminal libel at common law. Likewise, if a person is libeled by a document which is physically prepared and copied without the use of a computer system, such a person would also have to resort to the common law.

Conclusion

60 The Committee concludes that unless the language in the current draft of the Bill is amended, it will inevitably face challenge in the Courts.

May 14, 2024.

Bryan Walker

……..
Chairman

BARBADOS ASSOCIATION OF JOURNALISTS AND MEDIA WORKERS
YOUR EYES | YOUR EARS | YOUR VOICE

MAILING ADDRESS: #Franmar, Hillaby, St. Thomas, Barbados Email: barjambarbados@gmail.com

PRESIDENT
Ryan Broome
Tel: 246-230-3954

GENERAL SECRETARY
Michron Robinson
Tel: 246-233-9993

May 9th, 2024

WRITTEN SUBMISSION OF THE BARBADOS ASSOCIATION OF JOURNALISTS & MEDIA WORKERS (BARJAM) TO THE JOINT SELECT COMMITTEE ON GOVERNANCE AND POLICY MATTERS

The Barbados Association of Journalists & Media Workers (BARJAM) first wishes to express thanks to the Chair and Committee for its inclusion in this important process that gives ordinary citizens and civil society entities the opportunity to be a part of the legislative process.

With that said we recognize the intention of the Cybercrime Bill in a world where cyber-bullying and revenge porn are realities in a rapidly changing digital environment that has now added artificial intelligence software to the mix.

We believe the legislation can serve a useful purpose in better policing what can perhaps be easily described as an at times very chaotic online environment where almost anything seemingly goes.

However, we also believe we cannot lose sight of our existing laws which already safeguard some of these rights of our citizens.

Many of us in the media profession would have learned at some early point in our training that truth is an absolute defence to defamation and libel.

It is therefore our view that the impact of the Cybercrime legislation on freedom of expression as it relates to truth, should be no different than the impact of the defamation laws in the real world.

To put it in context and to use an everyday analogy, whatever views and opinions are freely and fairly expressed on the two most popular call-in programmes – Starcom's Brass Tacks or CBC's Talk Yuh Talk without being "cut" - should be equally allowed in the online environment.

Both of those media houses employ producers to "police" the live contributions with the use of a delay system, but their judgement in that ten or 20 second delay is primarily based on the standard that most media houses use for public comment. That standard is ultimately informed by our defamation and libel laws.

Some of those considerations could include: Is what the person has said a fair comment? Is it merely a personal attack without basis? Is it fair question or is this something is deliberately malicious that will result in us paying out a settlement?

To connect this scenario directly with the Bill, if we are to put truth in the context of the Malicious Communication section of the Bill, for example at 19 (3) which speaks of ridicule, contempt or embarrassment, in our layman's view it appears that the Cybercrime Bill could potentially be brought into conflict with that widely accepted legal position that truth is an absolute defence.

And while Section (5) states "the defences of truth, comment, triviality and privilege, whether absolute or qualified, provided for under the Defamation Act, Cap. 199 shall extend to a prosecution under subsection (3)," one wonders why there is a need to be specific in mentioning ridicule, contempt and embarrassment in the first place.

Section 5 essentially nullifies the need to have 19 (3) in the first place.

Moreover we believe it has also been one of the foremost points of contention in the public domain because of what is being inferred by its inclusion.

To put it another way, and to use the earlier analogy, if something is said on Brass Tacks or Talk Yuh Talk that can potentially ridicule, be contemptuous or embarrassing to a public figure for example, as long as it stands up to the standard of truth that is the ultimate test. That standard does not diminish in a digital environment so why mention it?

We believe 19 (3) represents a bridge too far in the attempt to have the legislation be all things to all people, particularly in a case where the relevant law already exists.

It is no surprise that this particular issue has raised as much concern as it has among members of the general public.

Unfortunately, some of that debate has become very emotive because there are those who believe they should be able to say anything about anyone, irrespective of truthfulness, in the digital environment.

We do not agree with that approach because members of the media have been subjected to such reckless and untrue attacks simply for doing their jobs.

No perceived legal freedom can be absolute in so far as it infringes on the rights of another person, not even freedom of expression.

We are not in support of an "anything goes" approach to public utterances on social media. However, we also believe if it is fair comment and within the four corners of the existing defamation laws then it should not be considered criminal.

In short, if we can have robust debate and constructive on any number of issues, economic political or social, in the real world on television and radio…and those discussions occasionally result in some hurt feelings without repercussions, then the standard should be no different in the digital environment.

We believe journalists in particular should be allowed to conduct their work fairly, without fear of prosecution or persecution.

We should also state here that the Cybersecurity Bill cannot be a stand-alone measure if democracy and justice are to reach as deep into the governance of our society as possible. With the contemplation of this piece of legislation, it must also follow that the promised Freedom of Information (FOI) legislation be enacted to bring balance to citizens' right to access and disseminate certain information that is for the public good. The FOI laws would help to extend the process of governance, rule of law and citizens' right to ensure greater transparency and accountability in the public affairs of the country. While the Cybersecurity Bill may seek to prevent people from using the internet to maliciously cause harm to other people, the FOI measure may be used to legitimately obtain information from authorized government sources [agencies] to, among other things, expose infelicities or wrong doing on the part of senior public figures.

CONCLUSION

Finally, as it relates to the penalties set out in the Bill, while the penalties listed in the Bill are considered maximum penalties and therefore subject to a judge's discretion, we believe there may be some room for review and amendment, given the specific nature of the offences vis a vis the Offences Against the Person Act.

For Online child sexual abuse, child pornography and child grooming and related offences the penalty of ten years or $100,000 is justified. It could perhaps even go higher given the sentencing discounting that is often used in our court system.

However, there are a few others where the penalties appear somewhat heavy when compared to the relevant crime, using the Offences Against the Person Act as a guide.

These include but are not limited to 'Interfering With Programme or Data', 'Disclosure of Access Code at Section 11.(2) Illegal Interception of Data' and Misuse of Devices.

The Illegal Access standard of five years or $50,000 seems more in line with an appropriate penalty for offences of this nature.

We believe the intent of this piece of legislation is well-meaning but ultimately it must seek to strike a balance that ensures those with ill-intent are meant to be appropriately penalized, while also ensuring that otherwise well-intentioned citizens are not inadvertently found to be in breach.

As far as media workers specifically are concerned, we want to ensure through this submission as much as the relevant laws provide, that the requisite freedoms currently associated with media reporting are not infringed upon in any way – whether in the real or digital world.

We once again thank you for the opportunity to be a part of the process.

-ENDS-

Ryan M Broome

President, BARJAM

Vice President: Emmanuel Joseph
Treasurer: Marlon Madden
Public Relations Officer: Deanzer Roberts
Floor Members: Trevor Thorpe, Vonardo Corbin & Kemar Holder

Our Motto: "Your eyes, Your ears, Your voice"

PUBLIC SECTOR REFORM
Making Barbados Work Better

MEMORANDUM

FROM: **OLIVER THOMAS**
PRINCIPAL STATE COUNSEL

TO: Director Acting
The Office of the Director of Public Prosecutions

DATE: June 13, 2024

SUBJECT: **Review of Cybercrime Bill (2024-01-29)**

Introduction:

The ***Cybercrime Bill*** (the Bill) consists of 33 sections. The object of the Bill is to provide for the combatting of cybercrime, protection of legitimate interests in the use and development of information technologies, the facilitation of international co-operation in computer related crimes and related matters. It contains 8 summary offences and 17 indictable offences.

Given the growing concern for the need to address cybercrime, this Bill is both timely and necessary. This concern is shared by international organizations such as the United Nations and the Council of Europe. This is the speed and anonymity of the Internet allows criminals to commit a range of crimes, from large-scale cyber-attacks to activities such as using malware, phishing and spam, or the use of crypto-currencies for illicit transactions. Further, technology can also facilitate serious organised crimes, such as terrorism and money laundering.

The Controversy:

The current opposition to the Bill relates to ss 19 and 20. These sections establish offences of malicious communications and cyber bullying respectively. The Barbados Bar Association's Report to the Joint Select Committee of Parliament has identified possible constitutional infringements resulting from the wording of s 19 (3) of the Bill. We agree that the use of

the word “embarrassment” under s 19 (3) of the Bill is an unlawful restriction on the right to freedom of expression.

In the sphere of malicious communications, embarrassment has never been a basis for criminal action against a person. Historically, a malicious communication was one which exposed a person hatred, contempt and ridicule. A a threat to a person’s life or safety was also required. In ***Batson v. R [1989] LRC (Crim) 525***, the appellant’s conviction for sending a threatening letter to the Governor-General of Barbados was upheld. Such communication was held to be interpreted objectively as a threat to a person. The ***Computer Misuse Act, Cap. 124B*** presently criminalises malicious communications. Objectively, the communication must cause the recipient or any other person to whom the sender intends the communication to be sent some annoyance, inconvenience, distress or anxiety.

The opposition to ss 19 and 20 of the Bill has constitutional dimensions as these offences make it likely that the fundamental right to freedom of expression will be contravened. Professor Thomas I Emerson in ***The System of Freedom of Expression*** asserted that 'the system of freedom of expression in a democratic society' is based on four premises:

1. freedom of expression facilitates self-fulfilment,
2. it is an essential tool for advancing knowledge and discovering truth,
3. it is a way to achieve a more stable and adaptable community, and
4. it permits individuals to be involved in the democratic decision-making process.

Section 20 of the Bill criminalizes the intentional use of a computer system to publish, broadcast or transmit data that is offensive, indecent, or menacing in character for the purpose of causing humiliation, embarrassment and other things. Section 20 will pass constitutional muster because the offence seeks to prohibit the dissemination of morally outrageous expressions. Such a restriction would be reasonably required in the interests of public safety and public morality.

On the other hand, s 19 (3), constitutes an unlawful contravention of the right to freedom of expression because it disproportionately restricts the dissemination of ideas in order to protect a person's reputation. The criminal law is not concerned with a complainant's particular susceptibility to feelings of deep hurt and offence.

Analysis:

The Bill has introduced several key offences which serve to enhance cybersecurity and to address some contemporary societal issues. Notably, the Bill prohibits cyberbullying, child pornography, child grooming, cyber-terrorism, online child sexual abuse and revenge porn. These offences will undoubtedly give relief to law enforcement when dealing with these crimes which are often committed against vulnerable persons.

The Constitution of Barbados - like the Constitutions of the other Commonwealth Caribbean countries - guarantees to every resident of the country the right to the enjoyment of his freedom of expression, which includes "'freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to disseminate information and ideas without interference (whether the dissemination be to the public generally or to any person or class of persons) and freedom from interference with his correspondence or other means of communication. In a system of governance founded on constitutional democracy, it is imperative that the competing interests of the state and of the individual are reconciled. This right is subject to lawful restrictions that are reasonably required in the interests of defence, public safety, public order, public morality or public health.

In ***Schenck v United States, 249 US 47 (1919), at 52*** Justice Oliver Wendell Holmes Jr. of the US Supreme Court set out the classic test for the justifiability of the abridgement of free speech. He stated that "the question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent.' Indeed, the "clear and present danger" test became the standard for First Amendment cases. the subsequent judgments of the United States Supreme

Court the test has been understood to mean to be 'clear and present danger'. The test of clear and present danger' has been used by the United States Supreme Court in many varying situations and has been adjusted according to varying fact situations. It appears to have been repeatedly applied as in ***Virginia v Black (2003) 155 L Ed 2d 535 at 551–553***. In its present form the clear and present danger test has been reformulated to say that: 'The constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.' The US Supreme Court made a further refinement so that the state may ban what is called a 'true threat' in ***Virginia v Black (2003) 538 US 343 at 344***:

> *' "true threats", eg, Watts v United States 394 US 705, 708 (per curiam), which encompass those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals … The speaker need not actually intend to carry out the threat. Rather, a prohibition on true threats protects individuals from the fear of violence and the disruption that fear engenders, as well as from the possibility that the threatened violence will occur … Intimidation in the constitutionally proscribable sense of the word is a type of true threat, where a speaker directs a threat to a person or group of persons with the intent of placing the victim in fear of bodily harm or death.'*

The criminal law identifies certain wrongful behaviour that society regards as deserving of punishment. People breaching the criminal law are labelled as criminals and are penalised by the state. Given these serious consequences, the criminal law is typically reserved for limited kinds of

wrongdoing. From an examination of the case law, embarrassment has never been a basis on which criminal liability could be founded.

With s 19 (3) drafted in its current form it is understandable that certain sections of the public may interpret the actions of the state as seeking to silence public dissent. The law historically never criminalized acts that had the potential to embarrass or humiliate persons. In relation to criminalized speech, the law is concerned with acts which cause a person to apprehend the immediate application of unlawful force or those which actually cause a person to suffer a (recognized) psychiatric illness: ***R v. Ireland, R v. Burstow [1998] AC 147***.

Criminal libel under ***s 34*** of the ***Defamation Act, Cap. 199*** may be committed by broadcast or in permanent form. Criminal liability is established when the libel vilifies the subject by bringing him into hatred, contempt, and ridicule. The libel must be shown beyond reasonable doubt to have attached to the target.

To be sure, the entire s 19 is not objectionable. Section 19 (1) and 19 (2) create lawful offences. It is the breadth of s 19 (3) which is objectionable. This is because the offence prohibits the dissemination of any image or words which causes or can cause a person to suffer ridicule, contempt or embarrassment. This offence goes beyond the scope of criminal libel which is essentially the precursor to this offence. The ingredients to the s 19 (3) offence is derived from ***Derry v. Peek (1889) 14 App.Cas. 337*** which was a landmark case and dealt with fraudulent misrepresentation. The House of Lords in that case held that an absence of honest belief is essential to constitute fraud. Lord Herschell defined fraudulent misrepresentation as a statement which is made either:

1. Knowing it to be false
2. Without belief in its truth or
3. Recklessly, careless as to whether it be true or false

Thus a fraudulent misrepresentation is a false statement which, when made, the representor did not honestly believe to be true. In ***Reynolds v. Times Newspapers [1998] 3 ALL ER 961***, the House of Lords considered the interaction between two fundamental rights: freedom of expression and

protection of reputation. The court held that a person would only be liable for a libellous statement relating to political information "if the writer knew the statement was not true or if he made the statement recklessly, not caring whether it was true or false, or if he was actuated by personal spite or some other improper motive."

Section 19 (5) of the Bill includes the defence of privilege. Lord Nicholls of Birkenhead summarized the core of the defence of qualified privilege in the following passage from ***Reynolds*** as follows:

> *"The essence of this defence lies in the law's recognition of the need, in the public interest, for a particular recipient to receive frank and uninhibited communication of particular information from a particular source."*

The defence of privilege under s 11 provides for the application of the defence of qualified privilege in respect of the publication of certain reports or matters referred to in the First Schedule to the ***Defamation Act***. But qualified privilege is defeated when the defendant has acted with malice. And malice may be established where the defendant has disseminated information recklessly, not caring whether it is true. Malice is also proven where the defendant acted with an improper motive such as to attack the defendant.

Understood in this way, where an "accused" person charged under s 19 (3) of the Bill disseminates any information for the purpose of insulting or embarrassing a person then the defence of qualified privilege would be defeated. The person would have no proper reason for disseminating the said information. In this sense, s 19 (3) can be justified. In ***Phillips and others v Boyce and another (2006) 71 WIR 14***, the Barbados Court of Appeal held that there were certain occasions when a person should be free to express himself even if another person was defamed by the publication, provided that the publisher was not actuated by malice. The categories of qualified privilege were not closed and every case would be governed by its own facts. The objective of the law was to achieve some balance between a person's right to freedom of expression and another person's interest in protecting a good reputation. There must exist between the maker of the

statement and the recipient some duty or interest in the making of the communication. Whether a person had a legal, social or moral duty to make a defamatory statement was a question of law, a judicial value judgment.

Additionally, ss 19 and 20 create summary offences. It is foreseeable that the Barbados Police Service could be inundated with reports of persons who claim to have been humiliated and/or embarrassed. Each of these cases will have to be investigated. Although the Bill provides for the defence of triviality, this does not prevent frivolous reports from being made. What will stop aggrieved persons from reporting school dramas and petty squabbles in the community? Indeed, the flood gates may have been blown wide open.

Oliver J. M. Thomas
Principal State Counsel

DOCUMENTS CONSULTED

No. 9 of 2014

VIRGIN ISLANDS

COMPUTER MISUSE AND CYBERCRIME ACT, 2014

ARRANGEMENT OF SECTIONS

Section

I Assent

(Sgd.) Boyd McCleary, CMG, CVO,
Governor.

31st July, 2014-

VIRGIN ISLANDS

No. 9 of 2014

AN ACT to provide for securing computer material and prohibit the unauthorised access, modification or any form of interference with such material or the misuse of computers and to make provision for other matters connected thereto.

[Gazetted 14th August, 2014]

ENACTED by the Legislature of the Virgin Islands as follows:

Preliminary

Short title and commencement.

1. This Act may be cited as the Computer Misuse and Cybercrime Act, 2014 and shall come into force on a date the Governor may, by Proclamation published in the *Gazette*, appoint.

Interpretation.

2. (1) In this Act, unless the context otherwise requires,

"computer" means, subject to subsection (2), an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility, including the internet, directly related to or operating in conjunction with such device or group of such interconnected or related devices;

"computer service" includes computer time, data processing and the storage or retrieval of data;

"data" includes material in whatever form stored, kept or maintained in or through the use of a computer, the whole or any part of a computer programme, and any representation of information or concepts in a form suitable for use in a computer, including a programme suitable to cause a computer to perform a function;

"financial services business" means any business that is licensed, recognised, registered, incorporated or otherwise approved under any financial services legislation outlined in Schedule 2 of the Financial Services Commission Act, 2001 or that is otherwise regulated by the Financial Services Commission;

"Minister" means the Minister responsible for the administration of this Act; and

"programme" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function, and a reference to a "programme" or "computer programme" includes any part of that programme or computer programme.

(2) The definition of "computer" in subsection (1) does not include

(a) an automated typewriter or typesetter;

(b) a portable hand-held calculator;

(c) a similar device which is non-programmable or which does not contain any data storage facility; and

(d) such other device as the Minister may, by Order published in the *Gazette*, prescribe.

(3) For the purposes of this Act, a person secures access to a programme or data held in a computer if, by causing the computer to perform any function, he or she

(a) alters or erases the programme or data or any part thereof,

(b) copies or moves the programme or data or any part thereof to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held,

(c) uses the programme or data or any part thereof, or

(d) causes the programme or data or any part thereof to be output from the computer in which it is held, whether by having it displayed or in any other manner,

and references to access to a programme or data and to an intent to secure such access shall be construed accordingly.

(4) For the purposes of subsection (3) (c), a person uses a programme if the function he or she causes the computer to perform

(a) causes the programme to be executed; or

(b) is itself a function of the programme.

(5) For the purposes of subsection (3) (d), the form in which a programme or data is output and, in particular, whether or not it represents a form in which,

(a) in the case of a programme, it is capable of being executed, or

(b) in the case of data, it is capable of being processed by a computer,

is immaterial.

(6) For the purposes of subsections (3) (d) and (5), the term "output", in relation to a computer, programme or data, means a statement or representation, whether in written, printed, pictorial, graphical or other form, purporting to be a statement or representation of fact

(a) produced by a computer; or

(b) translated from a statement or representation so produced.

(7) For the purposes of this Act, access of any kind by a person to any programme or data held in a computer is unauthorised or done without authority if the person

(a) is not himself or herself entitled to control access of the kind in question to the programme or data; and

(b) does not have consent to access of the kind in question to the programme or data from a person who is so entitled; or

(c) is not acting pursuant to a power or function he or she is lawfully entitled to exercise or perform under this Act or the Telecommunications Act.

(8) A reference in this Act to a programme or data held in a computer includes a reference to any programme or data held in any removable storage medium which is for the time being in the computer, and a computer is to be regarded as containing any programme or data held in any such medium.

(9) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer,

(a) a programme or data held in the computer concerned is altered or erased,

(b) a programme or data is introduced or added to its contents, or

(c) an act occurs which impairs the normal operation of any computer,

and any act which contributes towards causing such a modification shall be regarded as causing it.

(10) A modification referred to in subsection (9) is unauthorised if

(a) the person whose act causes it is not himself or herself entitled to determine whether the modification should be made; and

(b) the person does not have consent to the modification from any person who is so entitled.

Application of Act.

3. (1) The provisions of this Act apply in relation to any person, whatever his or her nationality or citizenship, within or outside the Virgin Islands.

(2) Where an offence under this Act is committed by a person

(a) in any place outside the Virgin Islands, or

(b) partly in the Virgin Islands and partly outside the Virgin Islands,

he or she may be dealt with as if the offence had been committed in the Virgin Islands.

(3) This Act applies if, in relation to the offence in question,

(a) the accused was in the Virgin Islands at the material time;

(b) the computer, programme or data was in the Virgin Islands at the material time; or

(c) the computer, programme or data though not in the Virgin Islands at the material time contained or related to data regarding a national security matter or a financial services business.

(4) This Act applies where, prior to the enactment and commencement of this Act, information had been acquired which would have constituted an offence under section 13 had this Act been in force at the material time, if such information is published after the coming into force of this Act.

Computer Misuse and Cybercrime Offences

Unauthorised access to computer material.

4. (1) A person commits an offence if

(a) he or she knowingly causes a computer to perform any function with intent to secure access to any programme or data held in the computer, or to enable any such access to be secured, or is reckless as to whether such access is secured; and

(b) the access he or she intends to secure, or to enable to be secured, is unauthorised.

(2) For the purpose of subsection (1), it is immaterial whether or not the intent is directed at

(a) any particular programme or data;

(b) a programme or data of any kind; or

(c) a programme or data held in any particular computer.

(3) A person who commits an offence under subsection (1) is liable

(a) on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding two years, or both; or

(b) on conviction on indictment to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years, or both.

(4) If any damage is caused as a result of an offence under this section, a person convicted of the offence is, in addition to any penalty imposed on him or her under subsection (3) (a) or (b), liable,

(a) in the case of a summary conviction, to a further fine not exceeding five thousand dollars; and

(b) in the case of a conviction on indictment, to a further fine not exceeding twenty-five thousand dollars.

(5) For the purpose of subsection (4), damage may relate, but not be limited, to a computer or any programme or data held in any computer.

Access with intent to commit or facilitate the commission of an offence.

5. (1) A person commits an offence if he or she accesses any programme or data held in a computer with the intention of

(a) committing an offence that is punishable by imprisonment for a term of twelve months or more; or

(b) facilitating the commission of an offence referred to in paragraph (a), whether by himself or herself or by any other person.

(2) A person may commit an offence under subsection (1) even if the facts are such that the commission of the offence referred to in subsection (1) (a) was impossible.

(3) For the purposes of this section, it is immaterial whether

(a) the access referred to in subsection (1) is authorised or unauthorised; or

(b) the offence referred to in subsection (1) (a) is committed at the same time when the access is secured or at any other time.

(4) A person who commits an offence under subsection (1) is liable

(a) on summary conviction to a fine not exceeding twenty-five thousand dollars or to imprisonment for a term not exceeding three years, or both; or

(b) on conviction on indictment to a fine not exceeding seventy-five thousand dollars or to imprisonment for a term not exceeding five years, or both.

Unauthorised modification of computer material.

6. (1) A person who does any act which he or she knows will cause or is likely to cause an unauthorised modification of the contents of any computer or is reckless as to whether such unauthorised modification is caused or is likely to be caused, commits an offence.

(2) For the purposes of subsection (1), it is immaterial

(a) whether or not the act in question is directed at

(i) any particular programme or data;

(ii) a programme or data of any kind; or

(iii) a programme or data held in any particular computer; or

(b) whether an unauthorised modification is, or is intended to be, permanent or temporary.

(3) A person who commits an offence under subsection (1) is liable

(a) on summary conviction to a fine not exceeding forty thousand dollars or to imprisonment for a term not exceeding five years, or both; or

(b) on conviction on indictment to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding seven years, or both.

(4) If any damage is caused as a result of an offence under this section, a person convicted of the offence is, in addition to any penalty imposed on him or her under subsection (3) (a) or (b), liable,

(a) in the case of a summary conviction, to a further fine not exceeding thirty thousand dollars; and

(b) in the case of a conviction on indictment, to a further fine not exceeding fifty thousand dollars.

(5) For the purpose of subsection (4), damage may relate, but not be limited, to a programme or data held in any computer, loss or delay occasioned by unauthorised modification of the contents of any computer, or dilution or compromise of a trade secret.

Unauthorised use or interception of computer service.

7. (1) A person commits an offence if he or she knowingly

(a) secures access without lawful authority to any computer purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or

(c) uses or causes to be used, directly or indirectly, a computer or any other device for the purpose of committing an offence under paragraph (a) or (b).

(2) For the purposes of subsection (1), it is immaterial whether or not the act in question is directed at

(a) any particular programme or data;

(b) a programme or data of any kind; or

(c) a programme or data held in any particular computer.

(3) A person who commits an offence under subsection (1) is liable

(a) on summary conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years, or both; or

(b) on conviction on indictment to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding ten years, or both.

(4) If any damage is caused as a result of an offence under this section, a person convicted of the offence is, in addition to any penalty imposed on him or her under subsection (3) (a) or (b), liable,

(a) in the case of a summary conviction, to a further fine not exceeding thirty thousand dollars; and

(b) in the case of a conviction on indictment, to a further fine not exceeding fifty thousand dollars.

(5) For the purpose of subsection (4), damage may relate, but not be limited, to a computer or any programme or data held in any computer.

Unauthorised obstruction of use of computer.

8. (1) A person commits an offence if he or she, knowingly and without lawful authority or lawful excuse, directly or indirectly

(a) interferes with, degrades, or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any programme or data stored in a computer.

(2) A person who commits an offence under subsection (1) is liable on

(a) summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding two years, or both; or

(b) on conviction on indictment to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years, or both.

(3) If any damage is caused as a result of an offence under this section, a person convicted of the offence is, in addition to any penalty imposed on him or her under subsection (2) (a) or (b), liable

(a) in the case of a summary conviction, to a further fine not exceeding twenty thousand dollars; and

(b) in the case of a conviction on indictment to a further fine not exceeding thirty thousand dollars.

(4) For the purpose of subsection (3), damage may relate, but not be limited, to a computer or any programme or data held in any computer.

Unauthorised disclosure of password, access code, etc.

9. (1) A person who, knowingly and without lawful authority, discloses any password, access code or any other means of gaining access to a programme or data held in any computer commits an offence if he or she made the disclosure

(a) with a view to gain;

(b) for an unlawful purpose;

(c) knowing that it will or is likely to cause wrongful loss to another person, or being reckless as to whether such wrongful loss is or is likely to be caused;

(d) knowing that it will or is likely to compromise or threaten the national security of the Virgin Islands, or being reckless as to whether such national security is or is likely to be compromised or threatened; or

(e) knowing that it will or is likely to result in the physical injury or abduction or kidnapping of another person or a member of his family or being reckless as to whether or not such physical injury or abduction or kidnapping results or is likely to result.

(2) A person who commits an offence under subsection (1) is, subject to subsection (3), liable on conviction on indictment to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding ten years, or both.

(3) Where a person is convicted under subsection (2) on account of a disclosure made with a view to gain pursuant to subsection (1) (a), whether such gain is pecuniary or otherwise and whether it is for himself or herself or some other person, he or she shall be liable

(a) to two times the fine prescribed in subsection (2) or to the amount of the gain received, whichever is higher; and

(b) to an additional term of imprisonment not exceeding five years.

(4) For the purposes of

(a) subsection (1)(e), it is immaterial whether the person or any member of his or her family who suffers physical injury or is abducted or kidnapped was, at the time of the physical injury or abduction or kidnapping, in the Virgin Islands or outside the Virgin Islands; and

(b) subsection (3), a person who is convicted shall be treated as having gained (or received a gain) from the commission of his or her offence if

(i) he or she or some other person has received the whole or any part of the gain agreed or anticipated; or

(ii) the gain is agreed or anticipated to accrue or be payable or be transferred at some period, or upon or after the occurrence of an event, in the future.

Acting unlawfully in relation to access given to a computer, programme or data.

10. (1) Where a person has access to a computer or to a programme or data held in any computer for a specified or general lawful purpose, he or she commits an offence if he or she, without lawful authority,

(a) copies, transfers, shares, alters, retains, disposes of, or in any manner deals with, the programme or data or any other information contained in that or any other computer; or

(b) grants another person access to the computer or programme or data.

(2) A person who commits an offence under subsection (1) is, subject to subsection (3), liable on conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fifteen years, or both.

(3) Where it is proven that the person who is convicted under subsection (2) has gained, whether pecuniarily or otherwise and whether for himself or herself or some other person, from the commission of his or her offence, he or she shall be liable

(a) to two times the fine prescribed in subsection (2) or to the amount of the gain received, whichever is higher; and

(b) to an additional term of imprisonment not exceeding five years.

(4) For the purposes of subsection (3), a person who is convicted shall be treated as having gained (or received a gain) from the commission of his or her offence if

(a) he or she or some other person has received the whole or any part of the gain agreed or anticipated; or

(b) the gain is agreed or anticipated to accrue or be payable or be transferred at some period, or upon or after the occurrence of an event, in the future.

Unlawfully making available device or data for commission of an offence.

11. (1) A person commits an offence if he or she, for the purpose of committing or facilitating the commission of, an offence under any of sections 4 to 10, produces or manufactures, possesses, procures for use, sells, imports, distributes or otherwise makes available, a password or any access code or a computer or any data or device designed or adapted for the commission of such offence.

(2) A person who commits an offence under subsection (1) is liable

(a) on summary conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years, or both; or

(b) on conviction on indictment to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding ten years, or both.

(3) Where a person, without lawful justification proof of which shall lie on him or her, is found in possession of

(a) more than one password or access code, or

(b) a computer or any data or device, designed or adapted to be capable of use in committing any of the offences referred to in subsection (1),

he or she shall be presumed to possess the password or access code, or the computer , data or device, with intent to commit an offence under subsection (1).

(4) Any computer, data or device designed or adapted for the commission of an offence as referred to in subsection (1) that has been seized shall be forfeited to the Crown or disposed of in such manner as the court considers fit.

Offences involving protected computer.

12. (1) Where a person obtains access to a protected computer in the course of committing an offence under section 4, 5, 6, 7, 8 or 10 (1), he or she shall, if convicted for the offence, be liable to three times the fine or term of imprisonment prescribed for that offence.

(2) Subsection (1) applies to an offence committed under section 10 (1) only if section 10 (3) does not apply in respect of that offence.

(3) For the purposes of subsection (1), a computer shall be treated as protected if, at the time of the commission of the offence, the person committing the offence knew, or ought reasonably to have known, that, or was reckless as to whether, the computer, or any programme or data contained in that or any other computer is used directly in connection with, or necessary for,

(a) the security, defence or international relations of the Virgin Islands;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) confidential educational material, such as examination material;

(d) the provision of services directly relating to communications infrastructure, financial services business, public utilities, public transportation or key public infrastructure; or

(e) the protection of public safety, including systems related to essential emergency services such as police, fire and rescue service, civil defence and medical services.

(4) The Minister may, by Order published in the *Gazette* and subject to a negative resolution of the House of Assembly, amend subsection (3) in such manner as he or she considers fit.

Unlawful Publication of Computer Data and Child Pornography

Publication of computer programme or data without lawful authority.

13. (1) A person commits an offence if he or she publishes, whether to another person or to the public and by whatever medium, information obtained, whether by himself or herself or by or through another person,

(a) in relation to a protected computer as provided in section 12; or

(b) information obtained from a computer, programme or data which he or she knows or ought reasonably to have known was obtained without lawful authority.

(2) A person who commits an offence under

(a) subsection (1) (a) is liable on conviction on indictment to a fine not exceeding five hundred thousand dollars or to

imprisonment for a term not exceeding fifteen years, or both; or

(b) subsection (1) (b) is liable on conviction on indictment to a fine not exceeding two hundred and fifty thousand dollars or to a term of imprisonment not exceeding seven years, or both.

(3) For the purposes of this section, "information" includes any data, text, image, sound, code, computer programme, software or database.

(4) This section shall not affect

(a) the provision of information

(i) in accordance with any other enactment; or

(ii) to a lawful authority for the purpose of initiating or advancing an investigation into the commission, or a reasonable suspicion of the commission, of an offence under the laws of the Virgin Islands; or

(b) the publication of information if the person publishing the information can establish that the publication is in the public interest of the Virgin Islands.

Using a computer for child pornography.

14. (1) A person commits an offence if he or she intentionally

(a) produces child pornography for the purpose of its publication through a computer;

(b) publishes child pornography through a computer; or

(c) possesses child pornography in a computer or on any computer data storage medium.

(2) A person who commits an offence under subsection (1) is liable on conviction on indictment to a fine not exceeding two hundred and fifty thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.

(3) It is a defence to a charge for an offence under subsection (1) (b) if the person establishes to the satisfaction of the court that the child pornography was for a *bona fide* scientific, research, medical or law enforcement purpose.

(4) It is a defence to a charge for an offence under subsection (1) (c) if the person establishes to the satisfaction of the court that the child pornography was

(a) for a *bona fide* scientific, research, medical or law enforcement purpose; or

(b) sent to him or her without any prior request made by him or her or on his or her behalf and that he or she did not keep it for an unreasonable time after he or she had become aware of it.

(5) For the purposes of this section,

(a) "child pornography" includes material that visually depicts

(i) a child engaged in sexually explicit conduct,

(ii) a person who appears to be a child engaged in sexually explicit conduct, and

(iii) a child in nudity in a sexually explicit manner,

and "child" has the meaning provided in section 2 of the Children and Young Persons Act, 2005; and

(b) "publish" includes

(i) distribute, transmit, disseminate, circulate, deliver, exhibit, procure, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(ii) have in possession or custody, or under control, for the purpose of doing an act referred to in sub-paragraph (i); or

(iii) print, photograph, film, copy or make in any other manner, whether of the same or of a different kind or nature, for the purpose of doing an act referred to in sub-paragraph (i).

(6) Where a person is charged under subsection (1) for an offence, the court may, whether or not the person has been convicted for the offence, make an order

(a) for the removal of the child pornography from the computer or any computer data storage medium in such manner as it may direct; and

(b) forfeiting to the Crown the computer used, and any other material associated with the use of the computer, to produce or publish the child pornography.

Miscellaneous

Inciting, aiding, etc. the commission of an offence under this Act.

15. A person commits an offence if he or she intentionally incites, solicits, attempts, aids or abets the commission of an offence under this Act and is liable on conviction to the penalty prescribed for the offence to which his or her action relates.

Offence by a body corporate.

16. (1) Where an offence under this Act is committed by a body corporate and the court is satisfied that a director, manager, secretary or other senior officer of the body corporate

(a) connived in the commission of the offence, or

(b) failed to exercise due diligence to prevent the commission of the offence,

the director, manager, secretary or other senior officer shall,

(i) in the case of paragraph (a), be liable on conviction to the penalty prescribed for the offence; and

(ii) in the case of paragraph (b), be liable on conviction to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years, or both.

(2) For the purposes of subsection (1), the term "body corporate" shall be construed to include a partnership and any other unincorporated body.

Order for compensation.

17. (1) Where a person is convicted of an offence under this Act, the court may, in addition to any penalty imposed on the person, order the person to pay a fixed sum as compensation to any person who has suffered loss as a result of the commission of the offence.

(2) An order made under subsection (1) is without prejudice to any other remedy which the person who has suffered loss may be entitled to under any other law.

(3) An order under subsection (1) may be made by the court on its own motion or upon the application of any person who has suffered loss as a result of the offence.

(4) An application for compensation by a person who has suffered loss may be made at any time before the court passes sentence on the person to whom the application relates.

Regulations.

18. (1) The Minister may make regulations in order to give effect to the purposes of this Act.

(2) Regulations made under subsection (1)

(a) may prescribe a fine not exceeding fifty thousand dollars for any offence created under the Regulations; and

(b) shall be subject to a negative resolution of the House of Assembly.

Passed by the House of Assembly this 29th day of July, 2014.

(Sgd) Delores Christopher,
Deputy Speaker.

(Sgd) Joann Vanterpool,
Deputy Clerk of the House of Assembly.

No. 9 of 2019

VIRGIN ISLANDS

COMPUTER MISUSE AND CYBERCRIME (AMENDMENT) ACT, 2019

ARRANGEMENT OF SECTIONS

Section

I Assent
(Sgd.) Augustus J. U. Jaspert,
Governor.
12th February, 2020

VIRGIN ISLANDS

No. 9 of 2019

An Act to amend the Computer Misuse and Cybercrime Act, 2014 (No. 9 of 2014).

[Gazetted 25th February, 2020]

ENACTED by the Legislature of the Virgin Islands as follows:

Short title.

1. This Act may be cited as the Computer Misuse and Cybercrime (Amendment) Act, 2019.

Section 2 amended. No. 9 of 2014

2. The Computer Misuse and Cybercrime Act, 2014 (referred to in this Act as "the principal Act") is amended in section 2 by

(a) inserting in their proper alphabetical order, the following definitions:

""mobile phone tracking" means the tracking of the current position of a mobile phone and includes location based services that discloses the actual coordinates of a mobile phone bearer;

"service provider" means

(a) a person who provides an information and communication service including the sending, receiving, storing or processing of the electronic communication or the provision of other services in relation to it

through a computer;

(b) a person who owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or

(c) any other person that processes or stores data on behalf of such electronic communication service or users of such service;

"subscriber information" means any information contained in any form that is held by a service provider, relating to subscribers of its services other than traffic data and by which can be established

(a) the type of communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; or

(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;

"traffic data" means any data relating to a communication by means of a computer, generated by a computer that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service;";

(b) replacing the definition of "computer service" with the following:

"computer service" includes provision of access to any computer or to any function of a computer, computer output, data processing and the storage or retrieval of data;".

Section 4 amended.

3. Section 4 of the principal Act is amended by replacing subsection (3) with the following:

"(3) A person who commits an offence under subsection (1) is liable

(a) on summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding seven years, or both; or

(b) on conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.".

Section 7 amended.

4. Section 7 of the principal Act is amended by replacing subsection (3) with the following:

"(3) A person who commits an offence under subsection (1) is liable

(a) on summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding seven years, or both; or

(b) on conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.".

Section 11 amended.

5. Section 11 of the principal Act is amended by replacing subsection (2) with the following:

"(3) A person who commits an offence under subsection (1) is liable

(a) on summary conviction to a fine not exceeding two hundred thousand dollars or

to imprisonment for a term not exceeding seven years, or both; or

(b) on conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.".

Section 14 amended.

6. Section 14(1) of the principal Act is amended

(a) by inserting the words "adopts or modifies" immediately after the word "produces";

(b) by replacing the words "child pornography" with the words "child abuse material" wherever they appear;

(c) in subsection (1),

(i) in paragraph (b), by deleting the word "or";

(ii) in paragraph (c), by replacing the full stop at the end thereof with a semicolon; and

(iii) by inserting after paragraph (c) the following new paragraphs:

"(d) cultivate, entice or induce a child to an online relationship with another child or an adult on a computer, for a sexually explicit act or in a manner that may offend a reasonable adult;

(e) facilitate abusing a child online; or

(f) record in an electronic form own abuse or that of others pertaining to sexually explicit act with a child.".

(d) by replacing subsection (5) (a), with the following:

"(a) "child abuse material" includes audio recordings, and material that visually depicts

(i) a child engaged in sexually explicit conduct;

(ii) a person who appears to be a child engaged in sexually explicit conduct; and

(iii) a child in the nude or in a sexually explicit manner,

and "child" has the meaning provided in section 2 of the Children and Young Persons Act, 2005; and".

Sections 14A to 14H inserted.

7. The principal Act is amended by inserting after section 14 the following new sections:

"Sending offensive messages through a computer.

14A. (1) A person commits an offence if he or she sends by means of a computer

(a) information that is grossly offensive or has menacing character;

(b) information which he or she knows is false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, he or she persists in doing so by such computer; or

(c) electronic mail or an electronic message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages.

(2) For the purpose of this section, the term "electronic mail" or "electronic message" means a message or information created or transmitted or received on a computer including attachments in text, images, audio, video and any other electronic record which may be transmitted with the message.

(3) A person who commits an offence under subsection (1) is liable

(a) on summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term

not exceeding seven years, or both; or

(b) on conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.

Electronic defamation.

14B. (1) A person commits an offence if he or she defames another person using a computer.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years, or both.

Electronic forgery.

14C. (1) A person commits an offence if he or she intentionally and unlawfully interfere with a computer or data held in a computer with the intention that the computer or the data is used to induce a person to accept the data held in the computer as genuine and by reason of so accepting it, to do or not to do any act to his or her own or any other person's prejudice or injury.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years, or both.

Electronic fraud.

14D. (1) A person commits an offence if he or she for gain, interferes with data or a computer

(a) to induce another person to enter into a relationship; or

(b) with intent to deceive a person,

which act is likely to cause damage or harm to that person or any other person.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years, or both.

Misuse of encryption.

14E. (1) A person commits an offence if he or she for the purpose of the commission of an offence or concealment of incriminating evidence, knowingly and willfully encrypts any incriminating communication or data contained in a computer relating to the offence or incriminating evidence.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years, or both.

Electronic stalking.

14F. (1) A person commits an offence if he or she, with intent to harass, intimidate, torment, or embarrass any other person, communicates by computer to such person or to a third party

(a) using any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act anonymously or repeatedly whether or not conversation occurs; or

(b) threatening to inflict injury on the person or property of the person communicated with or any member of his or her family or household.

(2) A person who commits an offence under subsection (1) is liable

(a) on summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding seven years, or both; or

(b) on conviction on indictment to a fine not exceeding five hundred thousand dollars or to imprisonment for a term not exceeding fourteen years, or both.

(3) An offence under this section may be

committed either at the place from which the communication was made or at the place where the communication was received.

Spoofing.

14G. (1) A person commits an offence if he or she establishes a website or send an electronic message with a counterfeit source

(a) with the intention that a visitor to a computer or recipient of an electronic message will believe it to be an authentic source; or

(b) to attract or solicit a person to a computer,

for the purpose of gaining unauthorised access to commit a further offence or obtain information which can be used for unlawful purposes.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding three years, or both.

Violation of privacy.

14H. (1) A person commits an offence if he or she, knowingly or without lawful excuse or justification, captures, publishes or transmits an image of a private area of another person, without his or her consent, under circumstances violating the privacy of that person.

(2) A person commits an offence if he or she, knowingly or without lawful excuse or justification, captures, publishes or transmits an image of a private area of a mentally or physically impaired person.

(3) A person who commits an offence under subsections (1) or (2) is liable

(a) on summary conviction to a fine not exceeding two hundred thousand dollars or to a term of imprisonment not exceeding seven years or to both; or

(b) on conviction on indictment to a fine not exceeding five hundred thousand dollars or to a term of imprisonment not exceeding fourteen years or to both.

(4) For the purposes of this section

(a) "capture" means to videotape, photograph, film or record by any means;

(b) "private area" means the naked or undergarment clad genitals, pubic area, buttocks, or female breast;

(c) "publishes" means reproduction in the printed or electronic form and making it available publicly;

(d) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that

(i) he or she could disrobe in privacy, without being concerned that an image or his or her private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.".

Sections 14I to 14S inserted.

8. The principal Act is amended by inserting the following new heading and sections:

"INVESTIGATIONS AND PROCEDURES

Preservation order.

14I. (1) A police officer may apply to a court for an order for the expeditious preservation of data that has been stored or processed by means of a computer, where there are reasonable grounds to believe that the data is vulnerable to loss or modification and where such data is required for the purposes of a criminal investigation or the prosecution of an offence.

(2) For the purposes of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) shall remain in force

(a) until such time as may reasonably be required for the investigation of an offence;

(b) where prosecution is instituted, until the final determination of the case; or

(c) until such time as the court may deem necessary.

Disclosure of pre**s**erved data order.

14J. (1) A police officer may, for the purposes of a criminal investigation or the prosecution of an offence, apply to a court for an order for the disclosure of

(a) any preserved data, irrespective of whether one or more service providers were involved in the transmission of the data;

(b) sufficient data to identify the service providers and the path through which the data was transmitted; or

(c) the electronic key enabling access to or the interpretation of data.

(2) For the purposes of this section, "electronic key" in relation to any data or other computer output, means any code, password, algorithm the use of which

(a) allows access to the data or output; or

(b) facilitates the putting of the data or output into intelligible form;

Production order.

14K. (1) If the disclosure of data is required for the purpose of a criminal investigation or the prosecution of an offence, a police officer may apply to a court for an order compelling

(a) a person to submit specified data in that person's possession or control, which is stored in a computer;

(b) a service provider offering its services to submit subscriber information in relation to the services in that service provider's possession and control.

(2) Where any material to which an investigation relates consists of data stored in a computer, disc, cassette, or on microfilm or preserved by any mechanical or electronic device, the request for disclosure of data mechanical or electronic device shall require the person to produce or give access to it in a form in which it can be taken away and in which it is visible, audible, and legible as relevant.

(3) A person or service provider who refuses to produce the information under subsection (1) commits an offence and is liable on conviction to a fine not exceeding one hundred thousand dollars.

Powers of access, search and seizure for the purpose of investigation.

14L. (1) Where a police officer has reason to believe that stored data would be relevant for the purposes of an investigation or the prosecution of an offence, the police officer may apply to a court for the issue of a warrant to enter any premises to access, search and seize that data.

(2) In the execution of a warrant under subsection (1), the powers of a police officer shall include the power to

(a) access, inspect and check the operation of a computer;

(b) use or cause to be used a computer to search any data contained in or available on the computer;

(c) access any information, code or technology which has the capability of transforming or unscrambling encrypted data contained or

available to a computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which is disclosed in the course of the lawful exercise of the powers under this section;

(d) require a person in possession of the decryption information to grant the police officer access to such decryption information necessary to decrypt data required for the purpose of investigating the offence;

(e) seize or secure a computer.

(3) In the execution of a warrant under subsection (1), a police officer may be accompanied by professionals or experts as necessary to carry out the technical aspects of the search and seizure of the data.

(4) A person commits an offence if he or she knowingly or without lawful excuse

(a) obstructs a police officer in the exercise of the police officer's powers under this section; or

(b) fails to comply with a request made by a police officer under this section.

(5) A person who commits an offence under subsection (4) is liable on conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding one year, or both.

Real time collection of traffic data.

14M. Where a police officer has reasonable grounds to believe that any data would be relevant for the purposes of investigation and prosecution of an offence, the police officer may apply to a court for an order

(a) allowing the collection or recording of traffic data, in real time, associated with specified communications transmitted by

means of a computer; or

(b) compelling a service provider, within its technical capabilities to effect such collection and recording referred to in paragraph (a) or assist the police officer to effect such collection and recording.

Mobile phone tracking in emergencies.

14N. (1) A mobile phone service provider shall provide mobile phone tracking to the law enforcement agencies upon request in cases of emergencies with respect to the mobile phone of a person involved in such emergency.

(2) For the purposes of this section, "cases of emergency" include road accidents, missing persons and the pursuit of suspects involved in murder, rape or kidnapping.

(3) A mobile phone provider who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding twenty five thousand dollars.

Record of and access to seized items.

14O. (1) Where any computer or data is seized or rendered inaccessible in the execution of a warrant under section 14K, the person who executed the warrant shall, at the time of the search, or as soon as possible thereafter

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of the list to the person to whom the warrant is addressed or the occupier of the premises on which the warrant is executed.

(2) Subject to subsection (3), the police officer who executed the warrant or another authorised person shall, on request,

(a) permit a person who had the custody or control of the computer or data, or someone acting on their behalf to access and copy data on the computer data on the; or

(b) give the person a copy of the data.

(3) The police officer or authorised person may refuse to give access or provide copies of the data if he or she has reasonable grounds for believing that giving access, or providing the copies would

(a) constitute a criminal offence; or

(b) prejudice

(i) the investigation in relation to which the warrant was issued;

(ii) another ongoing investigation; or

(iii) any criminal proceedings that may be brought in relation to any investigation referred in subparagraph (i) or (ii).

Arrest without warrant.

14P. A police officer may, without a warrant, arrest a person reasonably suspected of committing an offence under this Act.

Deletion.

14Q. A court may, on application by a police officer and on being satisfied that a computer contains indecent data order that the indecent data be

(a) no longer stored on or be made available through the computer; or

(b) deleted or destroyed; and

(c) recorded and preserved by the police for the purposes of prosecution.

Limited use of data and information.

14R. A person shall not use or disclose data obtained pursuant to sections 14I, 14J, 14K, 14L, 14M and 14N for any purpose other than that for which the data was originally sought except

(a) in accordance with any other enactment;

(b) in compliance with an order of the court;

(c) where the data is required for the purpose of preventing, detecting or investigating offences or apprehending or prosecuting offenders;

(d) for the prevention of injury or other damage to the health of a person or serious loss or damage to property; or

(e) in the public interest.

Limitation of liability for service provider.

14S. (1) A service provider shall not be liable for any actions taken or any information provided or disclosed to the Police or other law enforcement agencies in accordance with sections 14I, 14J, 14K, 14L, 14M and 14N.

(2) A service provider who without lawful authority discloses

(a) the fact that an order under this Act has been made; or

(b) anything done under the order; or

(c) any data collected or recorded under the order,

commits an offence and is liable on conviction on indictment to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five year, or both.".

Section 17A inserted.

9. The principal Act is amended by inserting immediately after section 17 the following new section:

"Forfeiture.

17A. (1) Where a person is convicted of an offence under this Act the court may, in addition to any penalty imposed on the person, order the forfeiture of any apparatus, article or thing which is the subject matter of the offence or is used in connection with the commission of the offence.

(2) In addition to making an order that obscene matter forming part of the subject matter of the offence is forfeited, the court shall, where appropriate, order that the obscene matter be

deleted from or no longer be stored or made available through the computer.".

Section 18 amended.

10. Section 18 subsection (2) of the principal Act is amended by

(a) inserting a new paragraph (b) which reads as follows:

"(b) may extend the meaning of "computer" or "service provider" as may be necessary for the purposes of this Act"; and

(b) by renumbering the existing paragraph (b) as paragraph (c).

Passed by the House of Assembly this 18th day of October, 2019.

(Sgd.) Julian Willock,
Speaker.

(Sgd.) Phyllis Evans,
Clerk of the House of Assembly.

THE OFFICIAL GAZETTE 13TH AUGUST, 2018
LEGAL SUPPLEMENT — A

GUYANA

ACT NO. 16 OF 2018

CYBERCRIME ACT 2018

I assent.

David Granger,
President.

2018·08·13

ARRANGEMENT OF SECTIONS

SECTION

PART II
CYBERCRIME OFFENCES

PART III
ENFORCEMENT

AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences and related matters.

AD.2018 Enacted by the Parliament of Guyana:-

PART I
PRELIMINARY

Short title.

1. This Act may be cited as the Cybercrime Act 2018.

Interpretation.

2. In this Act –

"child" means a person under the age of eighteen years;

"child pornography"-

(a) means any visual depiction, including any film, video, digital image, computer or computer-generated or modified image, animation or text, of –

(i) a child engaging in real or simulated explicit sexual activity;

(ii) a child in a sexually explicit pose;

(iii) parts of a child's body pasted, for sexual purposes, to visual representations of parts of an adult's body or vice versa;

(b) does not include any visual representation of a child's body produced or reproduced for the purpose of education, counselling, or promotion of reproductive health or as part of a criminal investigation and prosecution or civil proceedings or in the lawful performance of a person's profession, duties and functions;

(c) does not require proof of the actual identity of a child;

"computer programme" means electronic data which

represents instructions or statements that, when executed in a computer system, can cause the computer system to perform a function;

"computer system" –

(a) means a device or group of interconnected or related devices, which follows a computer programme or external instruction to perform automatic processing of electronic data; and

(b) includes, but is not limited to, a desktop computer, a laptop computer, a netbook computer, a tablet computer, a video game console, internet connected devices, a smart phone, a personal digital assistant, a smart television or a video camera;

"electronic data"-

(a) means any digital representation of–

(i) facts;

(ii) concepts;

(iii) machine-readable code or instructions; or

(iv) information, including text, audio, image or video,

that is in a form suitable for processing in a computer system and is capable of being sent, received or stored; and

(b) includes traffic data or a computer programme;

"electronic data storage medium" means anything –

(a) in which electronic data is capable of being stored; or

(b) from which electronic data is capable of being retrieved or reproduced,

with or without the aid of a computer system;

"function" in relation to a computer system includes logic, control, arithmetic, deletion, storage or retrieval, and

communication or telecommunication to, from or within a computer system;

"intercept" includes –

(a) listening to, viewing, or recording a function of a computer system; or

(b) acquiring the substance, meaning or purport of a function of a computer system,

by use of technical means, other than by the sender or an intended recipient;

"service provider" means-

(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or

(b) any public or private entity that processes or stores electronic data on behalf of such communication service or users of such service;

"sexual activity" includes –

(a) touching with any part of the body, which includes a part surgically constructed (in particular, through gender reassignment surgery), with anything else or through anything; or

(b) any other activity,

if a reasonable person would consider that –

(i) whatever its circumstances or any person's purpose in relation to it, it is because of its nature sexual; or

(ii) because of its nature it may be sexual and because of its circumstances or the purpose of any person in relation to it (or both) it is sexual; or

(c) sexual intercourse;

"subscriber information" means any information contained in the form of electronic data or any other form that is held by a service provider, relating to subscribers of its services and by which can be established-

(a) the type of communication service used, the technical provisions taken and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;

"security measure" includes passwords, access codes and encryption codes, hardware and software programme configuration and update settings, and other controls to detect or prevent any cybercrime offence;

"traffic data" means electronic data that–

(a) relates to a communication by means of a computer system;

(b) is generated by a computer system that is part of a chain of communication; and

(c) shows the communication's origin, destination, route, time, date, size, geographic location, duration or the type of underlying services.

PART II
CYBERCRIME OFFENCES

Illegal access to a computer system.

3. (1) A person commits an offence if the person intentionally, without authorisation or in excess of authorisation, or by infringing any security measure, accesses a computer system or any part of a computer system of another person.

(2) A person who commits an offence under subsection (1) is liable –

(a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or

(b) on conviction on indictment to a fine of five million dollars and to imprisonment for five years.

Illegal interception.

4. (1) A person commits an offence if the person intentionally and without lawful excuse or justification, intercepts –

(a) the transmission of electronic data or any communication of another person to, from or within a computer system; or

(b) any electromagnetic emission carrying electronic data from a computer system.

(2) A person does not commit an offence under subsection (1) if –

(a) the transmission is for use of the general public;

(b) the person is a party to the transmission, or one of the parties to the transmission has provided consent to such interception;

(c) the person is acting on behalf of a service provider and the interception either is necessary to provide the service, or to protect the rights and property of the service provider or its customers, consistent with the service provider's terms of reference;

(d) the transmission is intercepted in obedience to a warrant issued by a Judge under section 6 of the Interception of Communications Act;

Cap. 47:03

(e) the transmission is intercepted under the Interception of

Communications Act on the authority of a designated officer in the case of a national emergency or in responding to a case where approval for a warrant is impracticable having regard to the urgency of the case;

(f) for a lawful security purpose, the person intercepts a transmission that constitutes unauthorised access, or access in excess of authorisation, from a computer system owned by the person, or with the authorisation of the owner.

(3) A person who commits an offence under subsection (1) is liable–

(a) on summary conviction to a fine of five million dollars and to imprisonment for three years; or

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Illegal data interference.

5. (1) A person commits an offence if the person intentionally and without lawful excuse or justification–

(a) causes electronic data of another person to deteriorate;

(b) deletes electronic data of another person;

(c) alters or modifies electronic data of another person;

(d) copies or moves electronic data of another person to a different location within a computer system or to any electronic data storage medium;

(e) renders electronic data of another person meaningless, useless or ineffective;

(f) obstructs, interrupts or interferes with another person's lawful use of electronic data; or

(g) denies access to electronic data to a person who is authorised to access it.

(2) A person who commits an offence under subsection (1), is liable–

(a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Illegal acquisition of data.

6. A person who, intentionally and without lawful excuse or justification, acquires electronic data of another person commits an offence and is liable–

(a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Illegal system interference.

7. (1) A person commits an offence if the person intentionally and without lawful excuse or justification, hinders or interferes with –

(a) a computer system of another person; or

(b) another person's lawful use or operation of a computer system.

(2) A person who commits an offence under subsection (1) is liable –

(a) on summary conviction to a fine of three million dollars and imprisonment for three years; or

(b) on conviction on indictment to a fine of eight million dollars and imprisonment for five years.

(3) For the purposes of this section "hinder" includes–

(a) disconnecting the electricity supply to a computer system;

(b) causing electromagnetic interference to a computer system;

(c) corrupting a computer system; or

(d) damaging, deleting, deteriorating, altering or suppressing computer programme.

Illegal devices.

8. (1) A person commits an offence if the person intentionally and without lawful excuse or justification, possesses, procures for use, produces, sells, imports, exports, distributes, discloses or otherwise makes available –

(a) a device or a computer programme, that is designed or adapted; or

(b) a computer password, access code, encryption code or similar data by which the whole or any part of a computer system, electronic data storage medium or electronic data is capable of being accessed,

for the purpose of committing an offence under this Act or any other law.

(2) A person who commits an offence under subsection (1) is liable –

(a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Unauthorised granting of access to or giving of electronic data.

9. (1) A person commits an offence who, through authorised or unauthorised means, obtains or accesses electronic data which –

(a) is commercially sensitive or a trade secret;

(b) relates to the national security of the State; or

(c) is stored on a computer system and is protected against unauthorised access,

and intentionally and without lawful excuse or justification grants access to or gives the electronic data to another person, whether or not he knows that the other person is authorised to receive or have access to the electronic data.

(2) A person who commits an offence under subsection (1) is liable –

(a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Computer-related forgery.

10. A person who inputs, alters, deletes or suppresses electronic data, resulting in inauthentic data, with the intent that it be considered or acted upon by another person as if it were authentic, regardless of whether or not

the data is directly readable and intelligible, commits an offence and is liable–

(a) on summary conviction to a fine of three million dollars and to imprisonment for three years; or

(b) on conviction on indictment to a fine of five million dollars and to imprisonment for five years.

Computer-related fraud.

11. (1) A person commits an offence if the person –

(a) inputs, alters, deletes or suppresses electronic data; or

(b) interferes with the functioning of a computer system,

with the intent to defraud or deceive another person for the purpose of procuring an economic benefit for himself or another person.

(2) A person who commits an offence under subsection (1) is liable–

(a) on summary conviction to a fine of five million dollars and to imprisonment for five years; or

(b) on conviction on indictment to a fine of ten million dollars and imprisonment for ten years.

Offences affecting critical infrastructure.

12. (1) Notwithstanding the penalties set out in any other provision of this Act or any other law, where a person commits an offence under this Act or under any other law and the offence results in the incapacity or destruction of or interference with, electronic data, a computer system, or a computer network that–

(a) is exclusively for the use of critical infrastructure of the State; or

(b) affects the use, or impacts the operation, of critical infrastructure of the State,

that person is liable on conviction on indictment to a fine of twenty million dollars and to imprisonment for ten years.

(2) For the purposes of this section, "critical infrastructure" means any electronic data, computer system, or computer network so vital to the

State that the incapacity or destruction of, or interference with, such electronic data, computer system, or computer network would have a debilitating impact on –

(a) the security, defence or international relations of the State;

(b) the existence or identity of a confidential source of information relating to the enforcement of the criminal law of the State;

(c) the provision of services by the Office of the Director of Public Prosecutions and the Ministry of Legal Affairs;

(d) confidential educational material, such as examination materials;

(e) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or essential public infrastructure such as hospitals, courts, traffic lights, bridges, airports and seaports;

(f) the protection of public safety, including systems related to essential emergency services such as police, fire brigade services, civil defence and medical services;

(g) the provision of services of the Revenue Authority established under the Revenue Authority Act; or

Cap. 79:04

(h) the provision of services of the Bank of Guyana.

Identity-related offences.

13. (1) A person commits an offence if the person uses a computer system to –

(a) transfer, possess or use a means of identification of another person; or

(b) make use of the electronic signature or password of another person,

with the intent to commit an offence under this Act or under any other law.

(2) A person who commits an offence under subsection (1) is liable –

(a) on summary conviction to a fine of five million dollars and to imprisonment for three years; or

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Child pornography.

14. (1) A person commits an offence if the person intentionally –

(a) produces child pornography with the use of a computer system;

(b) offers or makes available, distributes or transmits child pornography through a computer system;

(c) procures or obtains child pornography through a computer system for himself or another person; or

(d) possesses child pornography in a computer system or on an electronic data storage medium.

(2) A person or a service provider who has knowledge of another person committing child pornography through a computer system shall report the commission of the child pornography to the Police.

(3) A person or a service provider who fails to comply with subsection (2) commits an offence.

(4) A person who commits an offence under subsection (1), or a person or a service provider who commits an offence under subsection (3), is liable –

(a) on summary conviction to a fine of ten million dollars and to imprisonment for five years; or

(b) on conviction on indictment to a fine of fifteen million dollars and to imprisonment for ten years.

Child luring.

15. (1) A person commits an offence if the person uses a computer system to -

(a) communicate with a child with the intent to induce the child to engage in sexual conversations or sexual activities; or

(b) arrange a meeting with a child with the intent of abusing or engaging in sexual activity with the child or producing child pornography, whether or not he takes any steps to effect such a meeting.

(2) A person or a service provider who has knowledge of another person committing child luring through a computer system shall report the commission of the child luring to the Police.

(3) A person or service provider who fails to comply with subsection (2) commits an offence.

(4) A person who commits an offence under subsection (1), or a person or a service provider who commits an offence under subsection (3), is liable –

(a) on summary conviction to a fine of three million dollars and to imprisonment for five years; or

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Publication or transmission of image of private area of a person.

16. (1) A person commits an offence if the person intentionally captures, stores in, publishes or transmits through a computer system, the image of the private area of another person without that other person's consent.

(2) A person who commits an offence under subsection (1), is liable –

(a) on summary conviction to a fine of three million dollars and to imprisonment for three years; and

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

(3) For the purposes of this section, "private area" means naked genitals, buttocks or female breasts.

Multiple electronic mail messages and fraudulent website.

17. (1) A person commits an offence if the person –

(a) intentionally initiates the transmission of multiple

electronic mail messages from or through a computer system; or

(b) with intent to deceive or mislead a recipient or service provider as to the origin of the message, uses a computer system to transmit or retransmit multiple electronic mail messages,

that causes harm to a person or damage to a computer system.

(2) A person commits an offence if the person intentionally falsifies the header information of an electronic mail message for the purpose of committing an offence under this Act or any other law.

(3) A person commits an offence if the person without lawful excuse or justification establishes a website, with the intent to deceive or mislead a visitor to the website as to the authenticity of the website, for the purpose of gaining unauthorised access to information to commit a further offence.

(4) A person who commits an offence under this section is liable–

(a) on summary conviction to a fine of three million dollars and to imprisonment for three years; and

(b) on conviction on indictment to a fine of five million dollars and to imprisonment for five years.

(5) For the purposes of this section, "multiple electronic mail messages" means unsolicited data messages, including electronic mail and instant messages sent to more than fifty recipients within twenty-four hours.

Offences against the State.

18. (1) A person commits an offence if the person, whether in or out of Guyana, intentionally publishes, transmits or circulates by use of a computer system, a statement or words, either spoken or written, a text, video, image, sign, visible representation, or other thing, that –

(a) advocates the use, without authority of law, of force as a means of accomplishing a governmental change within Guyana;

(b) incites, counsels, urges, induces, aids or abets any person to commit, participate in the commission of, or to conspire with another person to commit treason under section 314 or 317 of the Criminal Law (Offences) Act;

Cap. 8:01

(c) encourages, incites, induces, aids, abets, counsels any person to commit or to conspire with another person to commit any criminal offence against the President or any member of the Government;

(d) (i) encourages, entices, induces or motivates any person in or out of Guyana to join a terrorist group or to commit or participate in the commission of an offence of or in relation to terrorist financing under Part V of the Anti-Money Laundering and Countering the Financing of Terrorism Act; or

Cap.10:11

(ii) incites, urges, teaches or trains any person in or out of Guyana to commit or participate in the commission of a terrorist act or an offence under the Anti-terrorism and Terrorist Related Activities Act; or

No. 15 of 2015

(e) excites or attempts to excite ethnic divisions among the people of Guyana or hostility or ill-will against any person or class of persons on the ground of race.

(2) A person who commits an offence under subsection (1) shall be liable on conviction on indictment to imprisonment for five years.

(3) Where death of the President, any member of the Government or any other person occurs as a result of the commission of an offence under subsection (1), the person who commits the offence is liable on conviction on indictment to imprisonment for life.

(4) For the purposes of subsection (1), a statement or words, a text, video, image, sign, visible representation or other thing does not constitute an offence if it –

(a) expresses disapprobation of the measures of the Government

with a view to obtain their alteration by lawful means;

(b) expresses disapprobation of the administrative or other action of the Government;

(c) expresses that the President, any member of the Government or the Government has been misled or mistaken in their measures;

(d) points out errors or defects of the Government, Constitution or Parliament; or

(e) procures, by lawful means, the alteration of any matter of government.

Using a computer system to coerce, harass, intimidate, humiliate, etc. a person.

19. (1) A person commits an offence if the person, with intent to compel another person to do any act which the other person is not legally bound to do or to abstain from doing any act which the other person has a legal right to do, uses a computer system to publish or transmit electronic data that –

(a) intimidates the other person; or

(b) threatens the other person to use violence to him or a member of his family or injure his property or the property of his family.

(2) A person commits an offence if he uses a computer system –

(a) to publish or transmit electronic data that is obscene, vulgar, profane, lewd, lascivious or indecent with intent to humiliate, harass or cause substantial emotional distress to another person; or

(b) to repeatedly send to another person electronic data that is obscene, vulgar, profane, lewd, lascivious or indecent with intent to humiliate or harass the other person to the detriment of that person's health, emotional well-being, self-esteem or reputation.

(3) A person commits an offence if the person uses a computer system

to disseminate any information, statement or image, knowing the same to be false, that –

(a) causes damage to the reputation of another person; or

(b) subjects another person to public ridicule, contempt, hatred or embarrassment.

(4) A person who uses a computer system with the intent to extort a benefit from another person by threatening to publish electronic data containing personal or private information which can cause the other person public ridicule, contempt, hatred or embarrassment commits an offence.

(5) A person who commits an offence under this section is liable–

(a) on summary conviction to a fine of five million dollars and to imprisonment for three years; and

(b) on conviction on indictment to a fine of ten million dollars and to imprisonment for five years.

(6) In subsection (1) –

(a) "intimidate" means –

(i) to cause in the mind of a reasonable person an apprehension of injury to him or to any member of his family or to any of his dependants or of violence or damage to any person or property; or

(ii) to cause a person substantial emotional distress; and

(b) "injury" includes injury to a person in respect of his business, occupation, employment or other source of income, and includes an actionable wrong.

Infringement of copyright, patents and designs and trademarks.
4&5 ELIZ. 2 Cap. 74

S.I. No. 79 of 1966

20. A person who uses a computer system to infringe –

(a) the rights of the copyright owner under the Copyright Act 1956 as applied to Guyana with certain exceptions and modifications to form part of the law of Guyana by the Copyright (British Guiana) Order, 1966;

(b) the rights of the proprietor of the patent or the rights of the

proprietor of a registered design under the Patents and Designs Act; or

Cap. 90:03

(c) the rights of the proprietor of a registered trade mark under the Trade Marks Act,

Cap. 90:01

commits an offence and is liable on summary conviction to a fine of three million dollars and imprisonment for three years.

Corporate liability.

21. (1) Where a body corporate commits an offence under this Act, the body corporate is liable to the fine applicable in respect of the offence.

(2) Where a body corporate commits an offence under this Act and the court is satisfied that a director, manager, secretary, or other similar officer, of that body corporate-

(a) consented or connived in the commission of the offence; or

(b) failed to exercise due diligence to prevent the commission of the offence,

that director, manager, secretary, or other similar officer commits an offence.

(3) A person who commits an offence under subsection (2) is liable -

(a) on summary conviction to a fine of five million dollars and to imprisonment for three years; and

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

Attempt, aiding or abetting.

22. A person who intentionally –

(a) advises, incites, attempts, aids, abets, counsels, procures or facilitates the commission of any offence under this Act; or

(b) conspires with another person to commit an offence under this Act,

commits an offence and shall be punished for the offence as if he had committed the offence as a principal offender.

Use of computer system to commit

23. Where an offence under any other law, not provided for in this Act,

offence under any other law.

is capable of being committed by a person through the use of a computer system, that other law shall be deemed to provide that the offence may be committed by a person through the use of a computer system and a person who commits the offence through the use of a computer system shall be liable to a fine of four times the monetary penalty provided by that law and to the same custodial sentence.

Offences prejudicing investigation.

24. (1) A person who knows or has reasonable grounds to believe that an investigation in relation to an offence under this Act is being or is about to be conducted, commits an offence if he intentionally -

(a) makes a disclosure that is likely to prejudice the investigation; or

(b) falsifies, conceals, destroys or otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents or electronic data that are relevant to the investigation.

(2) A person does not commit an offence under subsection (1)(a) if-

(a) the person does not know or have reasonable grounds to believe that the disclosure is likely to prejudice the investigation;

(b) the disclosure is made in the exercise of a function under this Act or in compliance with a requirement imposed under or by virtue of this Act;

(c) the person is an attorney-at-law and the disclosure is -

(i) to a client in connection with the giving of legal advice to the client; or

(ii) to any person in connection with legal proceedings or contemplated legal proceedings,

but a disclosure does not fall within this paragraph if the disclosure is made with the intention of furthering a criminal purpose.

(3) A person does not commit an offence under subsection (1)(b) if the person –

(a) does not know or suspect that the documents or electronic data are relevant to the investigation; or

(b) does not intend to falsify, conceal, destroy or otherwise dispose of any facts disclosed by the documents or electronic data from any official carrying out the investigation.

(4) A person who commits an offence under subsection (1) is liable-

(a) on summary conviction to a fine of five million dollars and to imprisonment for three years; and

(b) on conviction on indictment to a fine of eight million dollars and to imprisonment for five years.

PART III
ENFORCEMENT

Service providers to store traffic data and subscriber information.

25. (1) Subject to subsection (2), a service provider shall store traffic data of subscribers for ninety days from the date on which the data is generated by a computer system.

(2) A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that traffic data is reasonably required for the purpose of a criminal investigation or criminal proceedings under this Act or any other law, may order a service provider to store traffic data of subscribers for a period of more than ninety days but not exceeding one year on a special case by case basis.

(3) The service provider shall keep subscriber information from the beginning of the service provision, and such information shall be kept for a period of ninety days after the service agreement has ended.

(4) A service provider who fails to comply with this section commits an offence and is liable on summary conviction to a fine of three million

dollars and to imprisonment for one year.

Extension of time for prosecution of an offence.

26. Notwithstanding the provisions of any written law prescribing the time within which proceedings for an offence punishable on summary conviction may be commenced, summary proceedings for an offence against this Act, or for attempting to commit, conspiring with another person to commit, or soliciting, inciting, aiding, abetting or counselling or causing or procuring the commission of, such an offence, or for attempting to solicit, incite, aid, abet, counsel or cause or procure the commission of such an offence, may be commenced within twelve months of the commission of the offence:

Provided that where an offence against this Act is punishable on summary conviction and on conviction on indictment, nothing in this section shall be deemed to restrict the power to commence, after the expiry of the aforesaid period of twelve months, proceedings for conviction on indictment for that offence or for any other act, relating to the offence, referred to in this section.

Jurisdiction.

27. (1) A court in Guyana shall have jurisdiction in respect of an offence under this Act where the act constituting the offence is carried out–

(a) wholly or partly in Guyana;

(b) by any person, whether in Guyana or elsewhere; or

(c) by a person on board a vessel or aircraft registered in Guyana.

(2) For the purposes of subsection (1)(a), an act is carried out in Guyana if–

(a) the person is in Guyana at the time when the act is committed;

(b) the person is outside of Guyana at the time when the act is committed, but –

(i) a computer system located in Guyana or electronic

data on an electronic data storage medium located in Guyana is affected by, or contains information about, the act; or

(ii) the transmission or effect of the act, or the damage resulting from the act, occurs, in whole or in part, within Guyana.

(3) Subject to subsection (1), a Magistrate's court has jurisdiction to hear and determine any offence under this Act, if–

(a) the accused was within the magisterial district at the time when he committed the offence;

(b) a computer system, containing any computer programme or electronic data which the accused used, was within the magisterial district at the time when the accused committed the offence; or

(c) harm or damage occurred within the magisterial district, whether or not paragraph (a) or (b) applies.

Search and seizure.

28. (1) A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that there are reasonable grounds for suspecting that-

(a) an offence under this Act has been or is about to be committed in any place; and

(b) evidence that such an offence has been or is about to be committed is in that place,

may issue a warrant authorising a police officer, with such assistance as may be necessary, to enter the place to search for and seize the evidence, including any computer system, electronic data storage medium or electronic data.

(2) If a police officer who is undertaking a search under this section has reasonable grounds to believe that–

(a) the electronic data sought is stored in another computer system or electronic data storage medium; or

(b) part of the electronic data sought is in another place within Guyana,

and such electronic data is lawfully accessible from or available to the first computer system or electronic data storage medium, the police officer may extend the search and seizure to that other computer system, electronic data storage medium or other place.

(3) In the execution of a warrant under this section, a police officer may, in addition to the powers conferred on him by the warrant–

(a) activate an onsite computer system or electronic data storage medium;

(b) inspect and check the operation of a computer system or electronic data storage medium;

(c) make and retain a copy of electronic data;

(d) remove electronic data from a computer system or render the computer system inaccessible;

(e) take a printout of output of electronic data;

(f) impound or similarly secure a computer system or part of it or an electronic data storage medium.

(4) A police officer who undertakes a search under this section shall secure any computer system or electronic data storage medium and maintain the integrity of the electronic data that is seized.

(5) The seizure of any evidence, including any computer system, electronic data storage medium or electronic data under this section shall be valid for a period of ninety days and may be extended for a further period of not more than one year by a Judge in Chambers.

(6) When the seizure is no longer necessary, or upon its expiry date, any computer system, electronic data storage medium or electronic data seized shall be immediately returned to the person to whom the warrant was addressed.

(7) Where a police officer in the execution of a warrant under this section decides to seize a computer system or an electronic data storage

medium, the police officer may, on the request of the person who is in possession or control of the computer system or electronic data storage medium, permit the person to make a copy of electronic data of the description and in the manner set out in subsection (8) from the computer system or electronic data storage medium.

(8) The electronic data shall –

(a) to the satisfaction of the police officer be vital and of urgent need to the person before the expiry date referred to in subsection (6) and unrelated to the offence; and

(b) be copied in the presence of the police officer onsite or at the place where the computer system is held in the custody of the police.

(9) For the purposes of this section seizure does not include the computer system or electronic data storage medium of a service provider unless the service provider is intentionally using his computer system to commit an offence under the Act.

Record of seized material.

29. (1) If a computer system or an electronic data storage medium is seized or rendered inaccessible in the execution of a warrant under section 28, the person who executed the warrant shall, at the time of the execution, or as soon as possible thereafter-

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of that list to –

(i) the person to whom the warrant is addressed; or

(ii) the occupier of the premises on which the warrant is executed.

(2) A person, who immediately before the execution of a warrant, had possession or control of a computer system or an electronic data storage medium seized, may request a copy of electronic data from the police officer who executed the warrant, and the police officer shall, as soon as is

reasonably practicable, comply with the request.

(3) Notwithstanding subsection (2), a police officer who seizes a computer system or an electronic data storage medium may refuse to provide a copy of electronic data if he has reasonable grounds for believing that providing a copy would-

(a) constitute or facilitate the commission of a criminal offence; or

(b) prejudice-

(i) the investigation in relation to which the warrant was issued;

(ii) another ongoing investigation; or

(iii) any criminal proceedings that may be brought in relation to any investigation mentioned in subparagraph (i) or (ii).

Assistance.

30. (1) A person who has knowledge about the functioning of a computer system or an electronic data storage medium, or security measures applied to protect electronic data, that is the subject of a search warrant shall, if requested by the police officer authorised to undertake the search, assist the police officer by –

(a) providing information that facilitates the undertaking of the search for and seizure of the computer system, electronic data storage medium or electronic data sought;

(b) accessing and using the computer system or electronic data storage medium to search electronic data which is stored in, or lawfully accessible from or available to, that computer system or electronic data storage medium;

(c) obtaining and copying electronic data; or

(d) obtaining an intelligible output from a computer system or an electronic data storage medium in such a format that is admissible for the purpose of legal proceedings.

(2) A person who fails, without lawful excuse or justification, to comply with subsection (1) commits an offence and is liable on summary

conviction to a fine of three million dollars and to imprisonment for one year.

Production order.

31. A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that electronic data, traffic data, a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings under this Act or any other law, may order–

(a) a person in Guyana who is in possession or control of a computer system or an electronic data storage medium, to produce, from the computer system or electronic data storage medium, specified electronic data or a printout or other intelligible output of the electronic data; or

(b) a service provider in Guyana to produce traffic data relating to information transmitted from a subscriber through a computer system or from other relevant persons, or subscriber information about a person who uses the service,

and give it to a specified person within a specified period.

Expedited preservation order.

32. (1) A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that there are reasonable grounds to believe that electronic data or traffic data that is reasonably required for the purpose of a criminal investigation, under this Act or any other law, is vulnerable to loss or modification, may make an order requiring a person in possession or control of electronic data or traffic data to preserve and maintain the integrity of the electronic data or traffic data for a period not exceeding ninety days.

(2) A Judge, on an *ex parte* application by a police officer of the rank of Superintendent or above, may order an extension of the period referred to in subsection (1) by a further specified period of ninety days or more but not exceeding one year on a special case by case basis.

Disclosure of traffic data order.

33. A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that there are reasonable grounds to believe that traffic data stored in a computer system or an electronic data storage medium is reasonably required for the purpose of a criminal investigation, under this Act or any other law, into a communication, may make an order requiring a person to disclose sufficient traffic data about the communication to identify –

(a) the service provider; or

(b) the path,

through which the communication was transmitted.

Confidentiality of order.

34. (1) A person who is the subject of an order under section 31, 32 or 33 shall keep confidential-

(a) the fact that an order has been made;

(b) the details of an order;

(c) anything done pursuant to an order; or

(d) any electronic data collected or recorded pursuant to an order.

(2) A person who intentionally and without lawful excuse or justification fails to comply with subsection (1) commits an offence and is liable on summary conviction to a fine of five million dollars and to imprisonment for three years.

Prohibition of disclosures.

35. (1) Except as provided in subsection (2), a person shall not disclose or deliver electronic data, traffic data or subscriber information or any other information acquired in the course of their duties under this Act to any other person.

(2) The provisions under subsection (1) shall not apply to any actions between a service provider and any other person permitted under any law, or performed for the benefit of investigating or prosecuting a person who has committed an offence under this Act.

(3) Any person who violates subsection (1) commits an offence and

shall be liable on summary conviction to a fine of five million dollars and to imprisonment for three years.

Protection of person aiding in enforcement of Act.

36. A person or service provider shall not be liable under a civil or criminal law for any actions taken or the disclosure of any electronic data or other information that may be disclosed pursuant to the enforcement of this Act.

Order for removal or disablement of data.

37. A Judge, if satisfied on an *ex parte* application by a police officer of the rank of Superintendent or above that a service provider or any other entity with a domain name server is storing, transmitting or providing access to electronic data in contravention of this Act or any other written law, may order the service provider or other entity with a domain name server to remove, or disable access to, the electronic data.

Remote forensic tools.

38. (1) Where a Judge is satisfied on *ex parte* application by a police officer of the rank of Superintendent or above, that there are reasonable grounds to believe that electronic data which is required for the purpose of a criminal investigation into an offence under this Act or any other law, cannot be collected without the use of a remote forensic tool, the Judge may authorise a police officer, with such assistance as may be necessary, to utilise a remote forensic tool for the investigation.

(2) An application made under subsection (1) shall contain the following information-

(a) the name, and if possible, the address, of the person who is suspected of committing the offence;

(b) a description of the targeted computer system;

(c) a description of the required tool, the extent and duration of its utilisation; and

(d) reason for the use of the tool.

(3) Where an application is made under subsection (1), the Judge may

order that a person or a service provider support the installation of the remote forensic tool.

(4) Where a remote forensic tool is utilised under this section –

(a) modifications to a computer system shall be limited to those that are necessary for the investigation;

(b) modification to a computer system shall be undone, so far as possible, after the investigation; and

(c) the police officer authorised under subsection (1) shall, as soon as possible thereafter, prepare a record of –

(i) the remote forensic tool used;

(ii) the time and date of the application;

(iii) the identification of the computer system and details of the modification undertaken; and

(iv) the information obtained.

(5) The police officer responsible for a criminal investigation in which a remote forensic tool is utilised under this section shall ensure that any information obtained by the utilisation of the remote forensic tool is protected against modification, unauthorised deletion and unauthorised access.

(6) An authorisation that is granted under this section shall cease to apply where -

(a) the electronic data sought is collected;

(b) there is no longer any reasonable ground for believing that the electronic data sought exists; or

(c) the conditions of the authorisation are no longer present.

(7) For the purposes of this section, "remote forensic tool" means an investigative software or hardware installed on or attached to a computer system that is used to perform a task.

Order for payment of compensation.

39. (1) Where a person is convicted of an offence under this Act and the court is satisfied that another person has suffered loss or damage because of the commission of the offence, the court may, in addition to any penalty

imposed under this Act, order the person convicted to pay a fixed sum as compensation to that other person for the loss or damage caused as a result of the commission of the offence.

(2) An order made under subsection (1) shall be without prejudice to any other remedy which the person who suffered the loss or damage may have under any other law.

(3) The court may make an order under subsection (1) of its own motion or upon the application of a person who has suffered loss or damage as a result of the commission of the offence.

(4) A person who makes an application under subsection (3) shall do so in accordance with rules of court before sentence is passed on the person against whom the order is sought.

Forfeiture order.

40. (1) Subject to subsection (2), where a person is convicted of an offence under this Act, the court that heard the criminal case may, upon the application of the Director of Public Prosecutions, order that any property–

(a) used for or in connection with; or

(b) obtained as a result of or in connection with,

the commission of the offence be forfeited to the State.

(2) Before making an order under subsection (1), the court shall give an opportunity to be heard to any person who-

(a) claims to be the owner of the property; or

(b) appears to the court to have an interest in the property.

(3) Where a person proves to the court that there is electronic data in a computer system or an electronic data storage medium forfeited which is useful to that person and unrelated to the offence committed, the Court shall make an order permitting the person to make a copy of that electronic data.

(4) Property forfeited to the State under subsection (1) shall vest in the State –

(a) if no appeal is made against the forfeiture order, at the end of the period within which an appeal may be made against

the forfeiture order; or

(b) if an appeal has been made against the forfeiture order, on the final determination of the matter, where the decision is made in favour of the State.

(5) Where property is forfeited to the State under this section, it shall be disposed of in such manner as the court orders.

Order for seizure and restraint regarding forfeiture.

41. Where an *ex parte* application is made by the Director of Public Prosecutions to a Judge and the Judge is satisfied that there are reasonable grounds to believe that there is in any building, place or vessel, any property in respect of which a forfeiture order under section 40 has been made, the Judge may issue–

(a) a warrant authorising a police officer to search the building, place or vessel for that property and to seize –

(i) that property if found; and

(ii) any other property in respect of which the police officer believes, on reasonable grounds, that a forfeiture order under section 40 ought to have been made; or

(b) a restraint order prohibiting any person from disposing of, or otherwise dealing with any interest in, the property, other than as may be specified in the restraint order.

Failure to comply with a court order.

42. If any person fails to comply with an order of the Court, the person commits an offence and shall be liable –

(a) to a fine of one million dollars and to imprisonment for one year; and

(b) a further daily fine for each day the offence continues, of not more than fifty thousand dollars until the relevant corrective action has been taken.

Evidence.

43. In any criminal proceeding under this Act or any other law –

(a) any electronic data or traffic data, generated, retrieved or reproduced from a computer system or from an electronic data storage medium, and whether in electronic or printed form; or

(b) any computer system or electronic data storage medium,

acquired in respect of any offence, shall be admissible as evidence.

Passed by the National Assembly on the 20th July, 2018.

S.E. Isaacs, A.A.,

Clerk of the National Assembly

(BILL No. 17/2016)

THE CYBERCRIMES ACT
(Act 31 of 2015)

ARRANGEMENT OF SECTIONS

PART IV—*General*

[The inclusion of this page is authorized by L.N. 104A/2019]

THE CYBERCRIMES ACT

Act 3 of 2010, 31of 2015.

[*21st December, 2015.*]

PART I—*Preliminary*

1. This Act may be cited as the Cybercrimes Act. Short title.

2.—(1) In this Act— Interpretation.

"computer" means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and—

(*a*) includes any data storage facility or electronic communications system directly connected to or operating in conjunction with such device or group of such interconnected or relates devices;

(*b*) does not include such devices as the Minister may prescribe by order published in the *Gazette*;

"computer service" includes provision of access to any computer or to any function of a computer, computer output, data processing and the storage or retrieval of any program or data;

"damages", for the purposes of sections 3(3), 4(4), 5(3), 6(5), 7(2), 8(2), 9(3) and 10(2), means any impairment to a computer, or to the integrity or availability of data, that—

(*a*) causes economic loss;

(*b*) modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;

(*c*) causes or threatens physical injury or death to any person;

(*d*) threatens public health or public safety; or

(*e*) causes or threatens physical damage to a computer;

"data" includes—

(*a*) material in whatever form stored electronically;

(*b*) the whole or part of a computer program; and

(*c*) any representation of information or of concepts in a form suitable for use in a computer, including a program suitable to cause a computer to perform a function;

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities, and the word "electronically" shall be similarly construed;

"electronic communications system" means a system for creating, generating, sending, receiving, storing, displaying or otherwise processing electronic documents or data;

"function", includes logic, control, arithmetic, deletion, storage, retrieval, and communication to, from or within a computer;

"key", in relation to any data or other computer output, includes any key, code, password, algorithm, authentication or authorization token, biometric identifier, gesture, or other data the use of which (with or without other keys)—

(*a*) allows access to the data or output; or

(*b*) facilitates the putting of the data or output into intelligible form;

"output", in relation to a computer, data or program, means a statement or representation, whether in written, printed, pictorial, graphical, auditory, or other form—

(*a*) produced by a computer; or

(*b*) accurately translated from a statement or representation so produced;

"program" or "computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function, and a reference to a program includes any part of that program.

(2) For the purposes of this Act, a person obtains access to any program or data held in a computer if the person causes a computer to perform any function that—

(*a*) alters or erases the program or data;

(*b*) copies or moves the program or data to any storage medium other than that in which the program or data is held or to a different location in the storage medium in which the program or data is held;

(*c*) causes the program or data to be executed;

(*d*) is itself a function of the program or data; or

(*e*) causes the program or data to be output from the computer in which it is held, whether by having the program or data displayed or in any other manner,

and references to accessing, or to an intent to obtain access to, a computer shall be construed accordingly.

(3) For the purposes of subsection (2)(*e*)—

(*a*) a program is output if the data of which it consists is output, and it is immaterial whether the data is capable of being executed;

(*b*) in the case of data, it is immaterial whether the data is capable of being processed by a computer.

(4) For the purposes of this Act, a person who accesses, modifies, or uses, any program or data held in a computer, or causes the computer to perform any function, does so without authorization if—

(*a*) he is not himself entitled to control the access, modification, use or function of the kind in question;

(*b*) he does not have consent for the access, modification, use or function of the kind in question from any person who is so entitled; and

(*c*) he is not acting pursuant to a power or function given to him under this Act or the *Interception of Communications Act*,

and the word "unathorised" shall be construed accordingly.

(5) A reference in this Act to any "program or data held in a computer" includes a reference to any program or data held in any removable data storage medium which is for the time being in the computer.

(6) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer—

(*a*) any program or data held in the computer concerned is altered or erased;

(*b*) any program or data is added to the contents of the computer concerned; or

(*c*) any act occurs which impairs the normal operation of any computer,

and any act which contributes toward causing such a modification shall be regarded as causing it.

(7) A modification referred to in subsection (6) is unauthorised if—

(*a*) the person whose act causes the modification is not himself entitled to determine whether the modification should be made; and

(*b*) that person does not have consent for the modification from any person who is so entitled.

PART II—*Offences*

Unauthorised access to computer program or data.

3.—(1) A person who knowingly obtains, for himself or another person, any unauthorized access to any program or data held in a computer commits an offence.

(2) The intent required for the commission of an offence under subsection (1) need not be directed at—

(*a*) any specifically identifiable program or data;

(*b*) a program or data of any specifically identifiable kind; or

(*c*) a program or data held in any specifically identifiable computer.

(3) A person who commits an offence under subsection (1) is liable upon—

(*a*) summary conviction before a Resident Magistrate to—

(i) in the case of a first offence, a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(*b*) conviction on indictment before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.

Access with intent to commit or facilitate commission of offence.

4.—(1) A person commits an offence if that person accesses any program or data held in a computer with the intent to—

(*a*) commit any offence punishable by imprisonment for a term that exceeds one year; or

(*b*) facilitate the commission of an offence referred to in paragraph (*a*), whether by himself or by any other person.

(2) A person may commit an offence under subsection (1) even if the facts are such that the commission of the offence referred to in subsection (1)(*a*) is impossible.

(3) For the purposes of this section, it is immaterial whether—

(*a*) the access referred to in subsection (1) is with or without authorization;

(*b*) the offence referred to in subsection (1)(*a*) is committed at the same time when the access is secured or at any other time.

(4) A person who commits an offence under subsection (1) is liable upon—

(*a*) summary conviction before a Resident Magistrate to—

(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(*b*) conviction on indictment before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.

Unauthorised modification of computer program or data.

5.—(1) A person who does any act which that person knows is likely to cause any unauthorized modification of the contents of any computer, commits an offence.

(2) For the purposes of subsection (1)—

(*a*) the act in question need not be directed at—

(i) any specifically identifiable program or data or type of program or data;

(ii) any program or data held in a specifically identifiable computer; and

(*b*) it is immaterial whether the modifications is, or is intended to be, permanent or temporary.

(3) A person who commits an offence under subsection (1) is liable upon—

(*a*) summary conviction before a Resident Magistrate to—

(i) in the case of a first offence, a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(*b*) conviction on indictment before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.

Unauthorised interception of computer function or service.

6.—(1) A person commits an offence if that person knowingly—

(*a*) secures unauthorized access to any computer for the purpose of obtaining, directly or indirectly, any computer service; or

(*b*) without authorization, directly or indirectly intercepts or causes to be intercepted any function of a computer.

(2) For the purposes of this subsection (1), the access or interception referred to need not be directed at—

(2) For the purposes of this subsection (1), the access or interception referred to need not be directed at—

(*a*) any specifically identifiable program or data or type of program or data; or

(*b*) any program or data held in a specifically identifiable computer.

(3) Subsection (1) shall not apply to interception permitted under the provisions of the Interception of Communications Act.

(4) For the purposes of this section, intercepting includes listening to or viewing, by use of technical means, or recording, a function of a computer or acquiring the substance, meaning or purport of any such function.

(5) A person who commits an offence under subsection (1) is liable upon—

(*a*) summary conviction before a Resident Magistrate to—

(i) in the case of a first offence, a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(*b*) conviction on indictment before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or

imprisonment for a term not exceeding ten years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.

Unauthorised obstruction of operation of computer.

7.—(1) A person may commits an offence if that person, without authorization or without lawful justification or excuse, willfully causes, directly or indirectly—

(*a*) a degradation, failure, interruption or obstruction of the operation of a computer; or

(*b*) a denial of access to, or impairment of, any program or data stored in a computer.

(2) A person who commits an offence under subsection (1) is liable upon—

(*a*) summary conviction before a Resident Magistrate, to—

(i) in the case of a first offence, a fine not exceeding three million dollars or to imprisonment for a term not exceeding three years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(*b*) conviction on indictment before a Circuit Court, to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or

imprisonment for a term not exceeding ten years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.

Computer related fraud or forgery.

8.—(1) A person may commits an offence if that person fraudulently, with intent to procure an advantage for himself or another person—

(*a*) causes loss of property to another person by any—

(i) input, alteration, deletion or suppression of data; or

(ii) interference with any function of a computer; or

(*b*) accesses any computer and inputs, alters, deletes or suppresses any data ("the original data") with the intention that the data, after such input, alteration, deletion or suppression (whether or not that data is readable or intelligible), be considered or acted upon as if that data were the original data.

(2) A person who commits an offence under subsection (1) shall be liable upon—

(*a*) summary conviction before a Resident Magistrate, to—

(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(*b*) conviction on indictment before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding ten years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding fifteen years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding twenty years.

Use of computer for malicious communication.

9.—(1) A person commits an offence if that person uses a computer to send to another person any data (whether in the form of a message or otherwise)—

(*a*) that is obscene, constitutes a threat or is menacing in nature; and

(*b*) with the intention to harass any person or cause harm, or the apprehension of harm, to any person or property,

but (for the avoidance of doubt) nothing in this section shall be construed as applying to any communication relating to industrial action, in the course of an industrial dispute, within the meaning of the Labour Relations and Industrial Disputes Act.

(2) An offence is committed under subsection (1) regardless of whether the actual recipient of the data is or is not the person to whom the offender intended the data to be sent.

(3) A person who commits an offence under subsection (1) shall be liable upon—

(*a*) summary conviction before a Resident Magistrate, to—

(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(*b*) conviction on indictment before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding ten years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding fifteen years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding twenty years.

Unlawfully making available devices or data for commission of offence.

10.—(1) A person commits an offence who, for the purpose of committing, or facilitating the commission of, an offence under any of sections 3 to 9, possesses, receives, manufactures, sells, imports, distributes, discloses or otherwise makes available—

(*a*) a computer;

(*b*) any key; or

(*c*) any other data or device,

designed or adapted primarily for the purpose of committing an offence under any of sections 3 to 9.

(2) A person who commits an offence under subsection (1) is liable upon—

(*a*) summary conviction before a Resident Magistrate, to—

(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;

(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;

(*b*) conviction before a Circuit Court to—

(i) in the case of a first offence, a fine or imprisonment for a term not exceeding ten years;

(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding fifteen years; or

(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding twenty years.

Offences related to protected computers.

11.—(1) Where a computer in respect of which an offence under any of sections 3 to 10 is committed is a protected

computer, the offender shall be tried on indictment in the Circuit Court and shall be liable upon conviction to a fine or imprisonment for a term not exceeding twenty-five years.

(2) For the purposes of subsection (1), "protected computer" means a computer which, at the time of the commission of the offence, the offender knows, or ought reasonably to know, is necessary for, or used directly in connection with—

(*a*) the security, defence or international relations of Jamaica;

(*b*) the existence or identity of a confidential source of information relating to the enforcement of the criminal law of Jamaica;

(*c*) confidential educational material, such as examination materials;

(*d*) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or essential public infrastructure such as hospitals, courts, toll roads, traffic lights, bridges, airports and seaports; or

(*e*) the protection of public safety, including systems related to essential emergency services such as police, fire brigade services, civil defence and medical services.

(3) The Minister may, by order published in the *Gazette* and subject to affirmative resolution, amend subsection (2) so as to add, vary or exclude any use.

Inciting, *etc.*

12. A person who intentionally incites, attempts, aids or abets the commission of any offence under any of sections 3 to 10 ("the substantive offence"), or conspires with another person to commit the substantive offence, commits an offence and shall be liable to the same penalty as applies to the substantive offence, and to be proceeded against and punished accordingly.

Offences prejudicing investigation.

13.—(1) This section applies if a person knows or has reasonable grounds to believe that an investigation in relation to an offence under this Part is being, or is about to be, conducted.

(2) The person commits an offence if the person—

(*a*) makes a disclosure that is likely to prejudice the investigation; or

(*b*) falsifies, conceals, destroys or otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents or data that are relevant to the investigation.

(3) A person does not commit an offence under subsection (2)(*a*) if—

(*a*) the person does not know or have reasonable grounds to believe that the disclosure is likely to prejudice the investigation;

(*b*) the disclosure is made in the exercise of a function under this Act or in compliance with a requirement imposed under or by virtue of this Act; or

(*c*) the person is an attorney-at-law and the disclosure falls within subsection (4).

(4) A disclosure falls within this subsection if it is a disclosure—

(*a*) to, or to a representative of, a client of the attorney-at-law in connection with the giving by the attorney-at-law of legal advice to the client; or

(*b*) to any person in connection with legal proceedings or contemplated legal proceedings,

but a disclosure does not fall within this subsection if the disclosure is made with the intention of furthering a criminal purpose.

(5) A person does not commit an offence under subsection (2)(*b*) if the person—

(*a*) does not know or suspect that the documents are relevant to the investigation; or

(*b*) does not intend to conceal any facts disclosed by the documents from any official carrying out the investigation.

(6) A person who commits an offence under subsection (2)is liable—

(*a*) on conviction before a Resident Magistrate, to a fine not exceeding three million dollars or imprisonment for a term not exceeding three years; or

(*b*) on conviction on indictment before a Circuit Court, to a fine or imprisonment for a term not exceeding ten years.

Offences by bodies corporate.

14.—(1) For the avoidance of doubt, where a body corporate commits an offence under this Act, the body corporate shall be liable to the fine applicable in respect of the offence.

(2) Where a body corporate commits an offence under this Act and the court is satisfied that a director, manager, secretary, or other similar officer, of that body corporate—

(*a*) connived in the commission of the offence, that director, manager, secretary, or other similar officer, shall also be liable to be proceeded against for the offence and punished accordingly; or

(*b*) failed to exercise due diligence to prevent the commission of the offence, that director, manager, secretary, or other similar officer, shall be liable—

(i) on conviction before a Resident Magistrate, to a fine not exceeding two million dollars or imprisonment for a term not exceeding two years; or

(ii) on conviction on indictment before a Circuit Court to a fine or imprisonment for a term not exceeding six years.

[The inclusion of this page is authorized by L.N. 104A/2019]

Compensation.

15.—(1) Where a person is convicted of an offence under this Part, the court may, in the same proceedings and in addition to any penalty imposed under this Part, order the person convicted to pay a fixed sum as compensation to any person who has suffered loss as a result of the commission of the offence.

(2) An order under subsection (1) shall be without prejudice to any other cause of action which the person who has suffered loss may have under any other law.

(3) The Court may make an order under subsection (1) of its own motion or upon the application of any person in accordance with subsection (4).

(4) A person who has suffered loss as a result of the commission of an offence under this Part may apply in accordance with rules of court for an order under subsection (1), at any time before sentence is passed on the person against whom the order is sought.

PART III—*Investigations*

Interpretation and scope of Part III.

16.—(1) In this Part—

(*a*) "computer material" includes—

(i) data;

(ii) a computer (computer A) or any part thereof;

(iii) any other computer (computer B) or any part thereof, if—

(A) data from computer A is available to computer B, or data from computer B is available to computer A; and

(B) there are reasonable grounds for believing that such data is stored in computer B; and

(iv) any data storage medium;

(*b*) the power to seize includes the power to—

(i) make and retain a copy of data, including by using on-site equipment;

(ii) render inaccessible, or remove, data in a computer; and

(iii) take a printout of, or otherwise reproduce or capture, the output of any computer or data.

(2) This Part shall apply for the purpose of investigations and enforcement proceedings in respect of offences under any law.

Preservation of data.

17.—(1) Where a constable is satisfied that—

(*a*) data stored in a computer or any data storage medium is reasonably required for the purposes of a criminal investigation; and

(*b*) there are reasonable grounds for suspecting that the data may be destroyed or rendered inaccessible,

the constable may, by notice in accordance with subsection (2) given to the person in possession or control of the computer or data storage medium (as the case may be), require the person to ensure that the data be preserved.

(2) The notice referred to in subsection (1) shall be in writing and shall specify—

(*a*) the name of the person in possession or control of the computer or data storage medium (as the case may be) or the address where the computer or data storage medium (as the case may be) is located;

(*b*) the period for which the data is required to be preserved, being a period not exceeding sixty days; and

(*c*) the requirements to be complied with for the preservation of the data.

(3) For the purposes of subsection (2), "address" includes a location, e-mail address, telephone number or other number or designation used for the purpose of identifying a computer or electronic communications system.

(4) The period specified under subsection (2), or in any previous order made under this subsection, may be extended, upon the order of a Resident Magistrate on an application without notice, for such further period as may be specified by the Resident Magistrate in the order.

(5) A person commits an offence if the person fails, without reasonable excuse, to comply with a requirement imposed on that person by a notice or order under this section.

(6) A person commits an offence if, in purported compliance with a requirement imposed on that person under a notice or order made under this section, the person—

(*a*) makes a statement that the person knows to be false or misleading in a material particular; or

(*b*) recklessly makes a statement that is false or misleading in a material particular.

(7) A person who commits an offence under subsection (5) or (6) is liable—

(*a*) upon conviction before a Resident Magistrate, to a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;

(*b*) upon conviction on indictment before a Circuit Court, to a fine or imprisonment for a term not exceeding seven years.

Search and seizure warrants.

18.—(1) A Resident Magistrate may issue a warrant under this subsection, if satisfied by information on oath that there are reasonable grounds to suspect that there may be in any place any computer material that—

(*a*) may be relevant as evidence in proving an offence; or

(*b*) has been acquired by a person for, or in, the commission of an offence or as a result of the commission of an offence.

(2) A warrant under subsection (1) shall authorize a constable, with such assistance as may be necessary, to enter the place specified in the warrant to search for and seize the computer material.

Record of seized material.

19.—(1) If any computer material is seized or rendered inaccessible in the execution of a warrant under section 18(1), the person who executed the warrant shall, during the execution, or as soon as possible thereafter—

(*a*) make a list of what has been seized or rendered inaccessible; and

(*b*) give a copy of the list to the person to whom the warrant is addressed or the occupier of the premises on which the warrant is executed.

(2) A person who, immediately before the execution of a warrant, had possession or control of data seized in the execution, may request a copy of the data from the constable who executed the warrant, and the constable shall, as soon as is reasonably practicable, comply with request if the conditions under subsection (3) are satisfied.

(3) The conditions referred to in subsection (2) are that providing the copy would not—

(*a*) constitute or facilitate the commission of a criminal offence; or

(*b*) prejudice—

(i) the investigation in relation to which the warrant was issued;

(ii) another ongoing investigation; or

(iii) any criminal proceedings that may be brought in relation to any investigation mentioned in sub-paragraph (i) or (ii).

(4) A person who executes a warrant under section 18(1) shall take all reasonable steps to preserve the computer material seized or rendered inaccessible.

(5) A person who contravenes subsection (4) commits an offence and is liable upon conviction before a Resident Magistrate, to a fine not exceeding three million dollars, or in default of payment thereof to a term of imprisonment not exceeding three years.

(6) Where a computer material is seized or rendered inaccessible in the execution of a warrant under section 18(1), a person commits an offence if that person—

(*a*) uses the data comprised in the computer material for any purpose otherwise than in accordance with this Act; or

(*b*) discloses such data other than for the purposes of this Act,

and is liable upon conviction before a Resident Magistrate to a fine not exceeding three million dollars or, in default of payment thereof, to a term of imprisonment not exceeding three years.

Forfeiture.

20.—(1) Where any computer material is seized pursuant to section 19, an order under subsection (2) or (4) may be made in respect of the computer material.

(2) Where—

(*a*) any person is convicted of an offence; and

(*b*) the court concerned is satisfied that—

(i) the person owns computer material used in the commission of the offence;

(ii) the owner of computer material permitted it to be used in the commission of the offence; or

(iii) the circumstances are otherwise are otherwise such that it is just to do so,

the court shall, upon the application of the Director of Public Prosecutions, order the forfeiture of the computer material used in the commission of the offence.

(3) On the application of the Director of Public Prosecutions before a Resident Magistrate's Court having jurisdiction in the area where the computer material is seized, or a Judge of the Supreme Court in Chambers, the Court or Judge may make an order in accordance with subsection (4) notwithstanding that the conditions mentioned in subsection (2) have not been satisfied.

(4) Where an application is made under subsection (3), the Court or Judge (as the case may be) may order the forfeiture of the computer material if the Court or Judge is satisfied that—

(*a*) the computer material has been abandoned; or

(*b*) the circumstances in which the computer material was seized give reasonable cause to suspect that it was being used or has been used for committing an offence under this Act,

and it is otherwise just to do so.

(5) Where the Director of Public Prosecutions intends to apply for an order under subsection (4), the Director of Public Prosecutions shall give to any person who, to the knowledge of the Director of Public Prosecutions was at the time of the seizure, the owner of the computer material, notice of the seizure and the intention to apply for a forfeiture order and the grounds therefor.

(6) Where the Director of Public Prosecutions is unable to ascertain the owner of, or any person having an interest in, any computer material to which this section applies, the Director of Public Prosecutions shall publish a notice in a daily newspaper in circulation throughout Jamaica, of the intention to apply for a forfeiture order, not less than thirty days prior to the application.

(7) Any person having a claim to any computer material seized under this Act may appear at the hearing of the application for forfeiture and show cause why such an order should not be made.

(8) Where, on the hearing of an application for forfeiture under subsection (3), no person appears before the Judge to show cause as mentioned in subsection (7), the computer material shall be presumed to have been abandoned.

(9) If, upon the application of a person prejudiced by an order made under subsection (2) or (4), the Court or Judge (as the case may be) is satisfied that it is just in the circumstances of the case to revoke or vary the order, the Court or Judge may—

(*a*) revoke or vary the order upon such terms and conditions, if any, as the Court or Judge considers appropriate; and

(*b*) without prejudice to the generality of paragraph (*a*), require the person to pay in respect of the storage, maintenance, administrative expenses, security and insurance of the computer material, such amount as may be charged or borne by the person in whose custody the computer material was kept.

(10) An application under subsection (9) shall be made within thirty days after the date of the forfeiture order or within such longer period, not exceeding six months from the date of the order, as the Court or Judge (as the case may be) may allow.

Production orders.

21.—(1) A Resident Magistrate, if satisfied on the basis of an application made by a constable, that any data or other computer output specified in the application is reasonably required for the purpose of a criminal investigation or criminal proceedings, may make an order under subsection (2).

(2) An order under this subsection may require a person in possession or control of the data or other computer output to produce it in intelligible form to the constable.

(3) Where a production order requires the person to whom it is addressed to produce any data or other computer output to produce it in intelligible form, that person—

(*a*) shall be entitled to use any key in his possession or control to obtain access to the data or output;

(*b*) shall be taken to have produced the data or output in intelligible form if—

(i) the person makes, instead, a disclosure of any key to the data or output; and

(ii) the data or output is produced in accordance with the order, with respect to the person to whom, and the time in which, the person was ordered to produce the data or output.

(4) Where a constable has reasonable grounds to believe that—

(*a*) a key to any data or other computer output is in the possession of any person; and

(*b*) the production of the key is necessary for the purposes of the investigation in relation to which—

(i) the constable makes, or intends to make, an application for a production order; or

(ii) a production order has been issued to the constable,

the constable may apply, to the Resident Magistrate for such ancillary order, as may be required in the circumstances, to be included in the production order.

(5) An application under subsection (4) may be made—

(*a*) in any case referred to in subsection (4)(*b*)(i), at the time of the application for the production order;

(*b*) in any case referred to in subsection (4)(*b*)(ii), at any time after the making of the production order.

(6) Where the Resident Magistrate grants an application under subsection (4), the Resident Magistrate shall—

(*a*) in the case of an application under subsection (5)(*a*), include the ancillary order in the production order;

(*b*) in the case of an application made under subsection (5)(*b*), vary the production order to include the ancillary order.

(7) The ancillary order shall—

(*a*) describe the data or other computer output to which it relates;

(*b*) specify the time by which the order is to be complied with, being a reasonable time in all the circumstances; and

(*c*) set out the production that is required by the order and the form and manner in which the production is to be made,

and any such order may require the person to whom it is addressed to keep secret the contents and existence of the order.

(8) In granting an ancillary order, the Resident Magistrate shall—

(*a*) take into account—

(i) the extent and nature of any other information, in addition to the data or computer output in question, to which the key is also a key;

(ii) any adverse effect that complying with the order might have on any lawful business carried on by the person to whom the order is addressed; and

(*b*) require only such production as is proportionate to what is sought to be achieved, allowing, where appropriate, for production in such manner as would result in the putting of the information in intelligible form other than by disclosure of the key itself.

(9) An ancillary order shall not require—

(*a*) the production of any key which—

(i) is intended to be used for the purposes only of generating electronic signatures; and

(ii) has not in fact been used for any other purpose; or

(*b*) the production of any data or other computer output to a person other than the constable or such other person as may be specified in the order.

(10) Where an ancillary order is addressed to a person who—

(*a*) is not in possession or control of the data or other computer output to which the order relates; or

(*b*) is incapable, without the use of a key that is not in the person's possession or control, of obtaining access to the data or other computer output or producing it in intelligible form,

the person shall be taken to have complied with the order if the person produces any key to the data or other computer output (as the case may be), that is in the person's possession.

(11) It shall be sufficient for the purpose of complying with an ancillary order for the person to whom it is addressed to produce only those keys the production of which is sufficient to enable the person to whom they are produced to obtain access to the data or other computer output concerned and to put it into intelligible form.

(12) Where—

(*a*) the production required by an ancillary order allows the person to whom it is addressed to comply with the order without producing all of the keys in the person's possession or control; and

(*b*) there are different keys or combinations of keys in the possession or control of that person the production of which would constitute compliance with the order,

the person may select which of the keys, or combination of keys, to produce for the purpose of complying with the order.

(13) Where an ancillary order is addressed to a person who—

(*a*) was in possession or control of the key but is no longer in possession or control of it;

(*b*) if the person had continued to have possession or control of the key, would be required by virtue of the order to produce it; and

(*c*) is in possession or control of information that would facilitate the obtaining or discovery of the key or the putting of the data or other computer output concerned into intelligible form,

that person shall produce to the person to whom that person would have been required to produce the key, all such information as is mentioned in paragraph (*c*).

(14) A constable who obtains an ancillary order shall ensure that such arrangements are made as are necessary for securing that—

(*a*) a key produced in pursuance of the order is used to obtain access to, or put into intelligible form, only data or other computer output in relation to which the order was made;

(*b*) every key produced in pursuance of the order is stored, for so long as it is retained, in a secure manner, and any records of such key are destroyed as soon as no longer needed to access the data or other computer output concerned or put it into intelligible form; and

(*c*) the number of—

(i) persons to whom the key is produced or otherwise made available; and

(ii) copies made of the key,

is limited to the minimum that is necessary for the purpose of enabling the data or other computer output concerned to be accessed or put into intelligible form.

(15) A constable who knowingly contravenes subsection (14) commits an offence and, upon conviction before a Resident Magistrate, is liable to a fine not exceeding one million dollars or imprisonment for a term not exceeding one year.

(16) A person commits an offence if the person fails, without reasonable excuse, to comply with a requirement imposed on that person by an order under this section.

(17) A person who commits an offence under subsection (16) is liable—

(*a*) upon conviction before a Resident Magistrate, to a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;

(*b*) upon conviction on indictment before a Circuit Court, to a fine or imprisonment for a term not exceeding seven years.

(18) In this section—

"electronic signature" means anything in electronic form that—

(*a*) is incorporated into, or otherwise logically associated with, any electronic information;

(*b*) is generated by the signatory or other source of the information; and

(*c*) is used for the purpose of facilitating, by means of a link between the signatory or other source of the information, the establishment of the authenticity of the information, the establishment of its integrity, or both;

"information" includes data, text, images, sounds, codes, computer programs, software and databases.

PART IV—*General*

Jurisdiction.

22.—(1) This Act applies in respect of conduct occurring—

(*a*) wholly or partly in Jamaica;

(*b*) wholly or partly on board a Jamaican ship or Jamaican aircraft;

(*c*) wholly outside of Jamaica and attributable to a Jamaican national; or

(*d*) wholly outside of Jamaica, if the conduct affects a computer or data—

(i) wholly or partly in Jamaica;

(ii) wholly or partly on board a Jamaican ship or Jamaican aircraft.

(2) In this section—

"Jamaican aircraft" has the meaning assigned to it by section 2 of the *Civil Aviation Act*;

"Jamaican national" means a person who—

(*a*) is a citizen of Jamaica;

(*b*) has a connection with Jamaica of a kind which entitles that person to be regarded as belonging to, or as being a native or resident of, Jamaica for the purposes of the laws of Jamaica relating to immigration; or

(*c*) is a company or other legal entity constituted in Jamaica in accordance with the laws of Jamaica;

"Jamaican ship" has the meaning assigned to it by section 2 of the *Shipping Act*.

Regulations.

23.—(1) The Minister may make regulations in order to give effect to the purposes of this Act.

(2) Notwithstanding section 29(*b*) of the *Interpretation*

Act, and subject to affirmative resolution, regulations made under this Act may provide for penalties up to a maximum of one million dollars, on summary conviction or conviction on indictment for contravention of the regulations.

Power to amend monetary penalties by order.

24. The Minister may, by order subject to affirmative resolution and published in the *Gazette*, amend any monetary penalty imposed by this Act or the maximum monetary penalty specified in section 23(2).

Review of Act after three years.

25. The provisions of this Act shall be reviewed by a Joint Select Committee of the Houses of Parliament after the expiration of three years from the date of commencement of this Act.

BELIZE:

CYBERCRIME ACT, 2020

ARRANGEMENT OF SECTIONS

No. 32 of 2020

I assent,

(SIR COLVILLE N. YOUNG)
Governor-General

5th October, 2020.

AN ACT to combat cybercrime by creating offences of cybercrime; to provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto.

(Gazetted 7th October, 2020)

BE IT ENACTED, by and with the advice and consent of the House of Representatives and the Senate of Belize and by the authority of the same, as follows:

Part I

Preliminary

1. This Act may be cited as the **Short title.**

CYBERCRIME ACT, 2020.

Interpretation.

2.–(1) In this Act–

"Central Authority" means the Central Authority designated under the Mutual Legal Assistance Act;

Act No. 8 of 2014.

"child" means a person under the age of eighteen years;

"child pornography" has the meaning assigned to it under the Commercial Sexual Exploitation of Children Act;

Act No. 3 of 2013.

"Court" means the Supreme Court acting in its criminal jurisdiction;

"communication" means–

(a) anything encrypted or unencrypted comprising of speech, music, sounds, visual images or data of any description; and

(b) encrypted or unencrypted signals serving for the impartation of anything–

(i) between persons, a person and a thing or between things; or

(ii) for the actuation or control of any apparatus;

"communication data" means any-

(a) encrypted or unencrypted data comprised in or attached to a communication whether by the sender or otherwise, for the purpose of a communication network by means of which the communication is transmitted;

(b) encrypted or unencrypted information, that does not include the contents of a

communication, other than data that falls within paragraph ***(a)***, that is made by a person–

(i) of any communication network; or

(ii) any part of a communication network in connection with the provision to or use by any person of any communication service;

(c) encrypted or unencrypted information that does not fall within paragraph ***(a)*** or ***(b)*** that is held or obtained by a person providing a communication service in relation to a person to whom the service is provided;

"communication network" means any wire, radio, optical or other electromagnetic system used to route switch or transmit communication;

"communication service" means a service that consists in the provision of access to and of facilities for making use of, any communication network, whether or not it is one provided by the person providing the service;

"computer data" means any representation of–

(a) facts;

(b) concepts;

(c) machine-readable code or instructions; or

(d) information, including text, audio, image or video,

that is in a form suitable for processing in a computer system and is capable of being sent, received or stored;

"computer programme" means computer data which represents instructions or statements that, when executed in a computer system, can cause the computer system to perform a function;

"computer system" means a device or group of interconnected or related devices, which follows a computer programme or external instruction to perform automatic processing of computer data, including a desktop computer, a laptop computer, a netbook computer, a tablet computer, a video game console, a smart phone, a personal digital assistant, or a smart television;

"damage" means any impairment to the integrity or availability of data, a program, a computer system, communication network or information;

"function" in relation to a computer system includes logic, control, arithmetic, deletion, storage or retrieval, and communication or telecommunication to, from or within a computer system;

"Minister" means the Minister with responsibility for national security;

"person" includes a natural or legal person, an educational or financial institution or any legal or other entity;

"security measure" means password, access code, encryption code or biometric information in the form of computer data and includes any means of limiting access to authorised persons or to secure recognition prior to granting access to communication data, a communication network, a computer system or computer data;

"service provider" means–

(a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; or

(b) any public or private entity that processes or stores computer data on behalf of a communication service or users of the service;

"subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services and by which can be established–

(a) the type of communication service used, the technical provisions taken and the period of service;

(b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information available on the basis of the service agreement or arrangement; or

(c) any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement;

"Storage Direction" means any Order of a court compelling a service provider to store and make available to a stipulated party a person's stored traffic data and subscriber information; and

"traffic data" means any communication data–

(a) identifying, or purporting to identify, any person, apparatus or location to or from which the communication that is, may be or may have

been transmitted, and "data" in relation to a postal article, means anything written on the outside of the postal article;

(b) identifying or selecting, or purporting to identify or select, apparatus through or by means of which the communication is or may be transmitted;

(c) comprising signals for the actuation of–

(i) apparatus used for the purpose of a communication network for effecting, in whole or in part, the transmission of any communication; or

(ii) any communication network in which that apparatus is comprised;

(d) identifying the data or other data as data comprised in or attached to a particular communication; or

(e) identifying a computer file or a computer programme, access to which is obtained or which is run by means of the communication,

to the extent only that the file or the programme is identified by reference to the apparatus in which it is stored, and a reference to traffic data being attached to a communication includes a reference to the data and the communication being logically associated with each other.

Part II

Cybercrime Offences

Illegal access to a computer system.

3.–(1) A person commits an offence who, intentionally accesses a computer system or any part of a computer system of another person –

(a) without authorisation or in excess of authorisation; or

(b) by infringing any security measure of the computer system.

(2) A person commits an offence who intentionally and without lawful excuse or justification continues to exceed the authorised access to the computer system of another person.

(3) A person who commits an offence under this section is liable on–

(a) summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years;

(b) conviction on indictment to a fine of five thousand dollars and to a term of imprisonment for five years.

Illegal access to computer data.

4.–(1) A person commits an offence who, without authorisation accesses the computer system of another person with the intention to duplicate or modify the data–

(a) without authorisation or in excess of authorisation; or

(b) by infringing a security measure.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) conviction to a fine of five thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of ten thousand dollars and to a term of imprisonment for five years.

Illegal data interference.

5.–(1) A person commits an offence who, intentionally and without lawful excuse or justification–

(a) damages the computer data of another person;

(b) obstructs, interrupts or interferes with another person's lawful use of computer data; or

(c) denies access to computer data to another person who is authorised to access the computer data.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) summary conviction to a fine of eight thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of twelve thousand dollars and to a term of imprisonment for five years.

Illegal system interference.

6. –(1) A person commits an offence who, intentionally and without lawful excuse or justification, seriously hinders or interferes with the functioning of the computer system of another person by inputting, transmitting, damaging, modifying or suppressing computer data.

(2) A person who commits an offence under sub-section (1), is liable- on–

(a) summary conviction to a fine of **ten** thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of fifteen thousand dollars and to a term of imprisonment for five years.

(3) For the purposes of this section "seriously hinders" includes–

(a) disconnecting the electricity supply to the computer system;

(b) causing electromagnetic interference to the computer system; or

(c) corrupting the computer system.

Illegal devices and codes.

7.–(1) A person commits an offence who, for the purpose of committing an offence under this Act or any other law, intentionally and without lawful excuse or justification, possesses, procures for use, produces, sells, imports or exports, distributes, discloses or otherwise makes available–

(a) a device or a computer programme, that is designed or adapted; or

(b) a security measure by which the whole or any part of a computer system or computer data is capable of being accessed.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of eight thousand dollars and to a term of imprisonment for five years.

Computer related forgery.

8. A person commits an offence who, intentionally inputs, modifies or suppresses computer data, regardless of whether or not the data is directly readable and intelligible, and the

input, modification or suppression causes the data to become inauthentic–

(a) is liable on summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years; or

(b) on conviction on indictment to a fine of five thousand dollars and to a term of imprisonment for five years.

Identity related fraud.

9.–(1) A person commits an offence who, with the intent to defraud or deceive another person for the purpose of procuring an economic benefit for the person or another–

(a) inputs, alters, deletes or suppresses computer data; or

(b) interferes with the functioning of a computer system.

(2) A person who commits an offence under sub-section (1), is liable on–

(a) summary conviction to a fine of five thousand dollars and to a term of imprisonment for five years; or

(b) conviction on indictment to a fine of ten thousand dollars and to a term of imprisonment for ten years.

Identity related theft.

10.–(1) A person commits an offence who, with the intent to assume the identity of another person, uses a computer system or computer data to–

(a) obtain, transfer, possess or use a means of identification of another person; or

(b) make use of the security measures of another person.

(2) A person who commits an offence under subsection (1), is liable on–

(a) summary conviction to a fine of five thousand dollars and to a term of imprisonment for five years; or

(b) conviction on indictment to a fine of ten thousand dollars and to a term of imprisonment for ten years.

Child luring.

11.–(1) A person commits an offence who, uses a computer system to communicate with a child with the intent to –

(a) induce the child to engage in a sexual conversation or sexual activity with the child; or

(b) encourage the child to produce child pornography; or

(c) arrange a meeting with a child for the purpose of abusing or engaging in sexual activity with the child, or producing child pornography, whether or not the person takes any steps to effect the meeting.

(2) A person who commits an offence under subsection (1), is liable on–

(a) summary conviction to a fine of ten thousand dollars and to a term of imprisonment for five years; or

(b) conviction on indictment to a fine of fifteen thousand dollars and to a term of imprisonment for ten years.

Publication or transmission of image of private area.

12.–(1) A person commits an offence who, without the explicit consent of another person, intentionally captures, stores in, publishes or transmits through a computer system, an image of a private area of the other person and is liable–

(a) on summary conviction to a fine of five thousand dollars and to a term of imprisonment for five years; or

(b) on conviction on indictment to a fine of ten thousand dollars and to a term of imprisonment for ten years.

(2) For the purposes of this section, "private area" means genitalia, buttocks or breasts.

(3) Notwithstanding the penalty under sub-section (1), a Court may, by Order prohibit the offender from using the internet or any computer system and impose any conditions on the offender as determined by the Court.

(4) An Order under sub-section (3) shall be for any period the Court considers appropriate, including any period of imprisonment imposed on the offender.

(5) A prosecutor or an offender may apply to the Court for a variation of any condition under the Order.

(6) Where the Court determines that there is a change in the circumstances of the case, the Court may vary the conditions of the Order.

No liability for service provider.

13.–(1) A service provider or a user of the service provider's service, shall not be deemed a publisher or speaker of any

information that is provided by another service provider or user.

(2) A service provider or user shall not be liable for–

(a) any action taken to enable or make available to a subscriber or user, the technical means to restrict access to any material described under paragraph *(b)*; or

(b) any action voluntarily taken in good faith to restrict access to or availability of material which the service provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not the material is constitutionally protected.

Service provider to store traffic data and subscriber information.

14.–(1) A service provider shall store and keep the traffic data of subscribers from the date on which the data is generated by a computer system until ninety days after the termination of a service agreement with a customer.

(2) A service provider who fails to comply with the requirements under sub-section (1), commits an offence and is liable on summary conviction to a fine of twenty thousand dollars and to a term of imprisonment for three year.

Using a computer system to coerce, harass, intimidate, etc. a person.

15. –(1) A person commits an offence who, with intent to compel another person to do or refrain from doing any act, uses a computer system to publish or transmit computer data that–

(a) intimidates the other person;

(b) threatens the other person with violence or damage to property; or

(c) threatens a member of the other person's family with violence.

(2) For the purposes of this section "intimidate" means –

(a) to cause in the mind of a reasonable person an apprehension of injury to the person, to a member of the person's family or a to dependant of the person, or of violence or damage to the person's property; or

(b) to cause a person substantial emotional distress.

(3) A person commits an offence who, uses a computer system to–

(a) publish or transmit computer data that is obscene, vulgar, profane, lewd, lascivious or indecent, with intent to–

(i) humiliate, harass or cause substantial emotional distress to another person; or

(ii) cause the other person to be subject to public ridicule, contempt, hatred or embarrassment; or

(b) repeatedly send to another person, computer data that is obscene, vulgar, profane, lewd, lascivious or indecent with intent to humiliate or harass the other person, and the humiliation or harassment is detrimental to the health, emotional well-being, self-esteem or reputation of the other person.

(4) A person commits an offence who, uses a computer system to disseminate any information, statement

or image, knowing the information, statement or image to be false, with the intent to cause–

(a) harm to the reputation of the other person; or

(b) the other person to be subject to public ridicule, contempt, hatred or embarrassment.

(5) A person commits an offence who, uses a computer system to threaten to publish computer data containing personal or private information of another person, with the intent to–

(a) extort a benefit from the other person; or

(b) cause the other person public ridicule, contempt, hatred or embarrassment.

(6) A person who commits an offence under this section is liable on–

(a) summary conviction to a fine of ten thousand dollars and to a term of imprisonment for five years; or

(b) conviction on indictment to a fine of fifteen thousand dollars and to a term of imprisonment for ten years.

Infringement of copyright, patents and designs and trademarks.

16.–(1) A person commits an offence who, uses a computer system to infringe on the rights of–

(a) a copyright owner;

(b) a proprietor of a patent;

(c) a proprietor of a registered design; or

(d) a proprietor of a registered trademark.

(2) A person who commits an offence under subsection (1), is liable on summary conviction to a fine of three thousand dollars and to a term of imprisonment for three years.

Attempt, aiding or abetting.

17.–(1) A person commits an offence who, intentionally–

(a) advises, incites, attempts, aids, abets, counsels, procures or facilitates the commission of any offence under this Act; or

(b) conspires with another person to commit an offence under this Act.

(2) A person who commits an offence under subsection (1), is liable for the offence as if the person is the principal offender.

Offences prejudicing investigation.

18.–(1) A person commits an offence who, knows or has reasonable grounds to believe that an investigation in relation to an offence under this Act is being or is about to be conducted, and who intentionally–

(a) makes a disclosure that is likely to prejudice the investigation; or

(b) falsifies, conceals, destroys or otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents or computer data that are relevant to the investigation.

(2) A person who commits an offence under subsection (1), is liable on–

(a) summary conviction to a fine of five thousand dollars and to a term of imprisonment for three years; or

(b) conviction on indictment to a fine of eight thousand dollars and to a term of imprisonment for five years.

(3) Notwithstanding sub-section (1), it is a defence under sub-section (1)(a) if–

(a) the accused does not know or have reasonable grounds to believe that the disclosure is likely to prejudice the investigation;

(b) the disclosure is made in the exercise of a function under this Act or in compliance with a requirement imposed under or by virtue of this Act;

(c) the accused is an attorney-at-law and the disclosure is–

(i) to a client in connection with the giving of legal advice to the client; or

(ii) to any person in connection with legal proceedings or contemplated legal proceedings.

(4) Notwithstanding sub-section (1), it is a defence under sub-section (1)***(b)*** if the accused –

(a) does not know or suspect that the documents or computer data are relevant to the investigation; or

(b) does not intend to falsify, conceal, destroy or otherwise dispose of any facts disclosed by the documents or computer data, from any official carrying out the investigation.

(5) Notwithstanding sub-section (2)*(c)(ii)*, a person commits an offence if the disclosure is made in furtherance of a criminal purpose.

PART III

Enforcement

***Ex-parte* application for Storage Direction.**

19.–(1) The Director of Public Prosecutions or Head of Prosecution Branch may in the prescribed form, make an *ex-parte* application for a Storage Direction.

(2) An application under sub-section (1), shall–

(a) be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following–

(i) the name of the investigating police officer;

(ii) the facts or allegations giving rise to the application, including the alleged offence;

(iii) sufficient information for the Court to make a determination on whether to grant or refuse the application;

(iv) the ground on which the application is made;

(v) full particulars of all facts and circumstances alleged, including–

(aa) where practical, a description of the nature and location of the facilities or computer from, or the premises at, which the traffic data and subscriber information are to be intercepted; and

(bb) the basis for believing that evidence relating to the ground on which the application is made will be obtained during the life/period of the Storage Direction;

(vi) where applicable–

(aa) whether other investigative procedures were applied and whether they failed to produce the required evidence;

(bb) the reason why any other investigative procedures may be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;

(vii) the requested duration of the Storage Direction;

(viii) whether any previous application was made for a Storage Direction in respect of the person, facility or premises, and the status of that other application;

(ix) where applicable, a description of the computer system to be targeted; and

(x) any other relevant directives issued by a Court in relation to the matter.

(3) Where a serious offence is being, has been or is likely to be committed for the benefit of, or at the direction of, or in association with, a person, a group of persons or syndicate involved in organised crime or groups classified

as criminal gangs, an application for a Storage Direction, shall not require the grounds under section 22(1)***(a)***.

(4) Where a Storage Direction is based on the ground of national security, the application shall be accompanied by written authorisation by Minister.

(5) Records relating to an application for a Storage Direction, renewal or modification of a Storage Direction, shall immediately upon the determination of the matter, be–

(a) sealed by the Court; and

(b) kept in the custody of the Court, in a place that is not accessible to the public, or in any other place as the Court determines fit.

(6) The records under sub-section (5) may be unsealed upon an order by the Court for the following purpose only–

(a) on an application for a further Storage Direction, in relation to the same matter; or

(b) for a renewal of a Storage Direction.

Scope and form of Storage Direction.

20.–(1) A Storage Direction shall direct the named service provider to–

(a) keep stored, at any place in Belize accurate records of–

(i) the traffic data and subscriber information of any person, facility or premises;

(ii) any computer system; or

(iii) any communication in the course of its transmission;

(b) store the traffic data for the period of time as stated in the Storage Direction; and

(c) submit the stored traffic data and subscriber information to a named police officer.

(2) A Storage Direction shall specify–

(a) the manner in which the data is to be stored and submitted to the police officer; and

(b) any other conditions or restrictions that relate to the traffic data.

(3) A Storage Direction may contain any ancillary provisions as may be necessary to secure its implementation in accordance with the provisions of this Act.

21. – (1) The Director of Public Prosecutions or Head Prosecution Branch may in the prescribed form, make an *ex-parte* application for Search and Seizure Warrant.

***Ex-parte* application for Search and Seizure Warrant.**

(2) An application under sub-section (1), shall–

(a) be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following–

(i) the name of the investigating police officer;

(ii) that there is reasonable grounds for suspecting that–

(aa) an offence under this Act or any other law has been or is about to be committed, in a specified place; and

(bb) evidence that the offence has been or is about to be committed, is in the specified place;

(iii) the facts or allegations giving rise to the application, including the alleged offence;

(iv) sufficient information for the Court to make a determination on whether to grant or refuse the application;

(v) the ground on which the application is made;

(vi) full particulars of all facts and circumstances alleged, including–

(aa) where practical, a description of the nature and location of the facilities or computer from, or the premises at, which the traffic data and subscriber information are to be intercepted; and

(bb) the basis for believing that evidence relating to the ground on which the application is made will be obtained during the duration of the Search and Seizure Warrant;

(vii) where applicable–

(aa) whether other investigative procedures were applied and

whether they failed to produce the required evidence; or

(bb) the reason why any other investigative procedures may be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;

(viii) The requested duration of the Search and Seizure Warrant;

(ix) whether any previous application was made for a Search and Seizure Warrant in respect of the person, facility or premises, and the status of that other application;

(x) where applicable, a description of the computer system to be targeted; and

(xi) any other relevant directives issued by a Court in relation to the matter.

(3) A Search and Seizure Warrant shall specify the place, or evidence to which it relates and authorise a police officer, with any assistance as the police officer deems necessary, to–

(a) enter and search any place; or

(b) to access, seize and secure any evidence, including any computer system or computer data.

(4) A police officer who executes a Search and Seizure Warrant under this section shall, secure the computer system or data and maintain the integrity of the data seized.

(5) In addition to any powers of a Search and Seizure Warrant under this section, a police officer when executing a Search and Seizure Warrant, has the following additional powers including–

(a) to activate an onsite computer system;

(b) inspect and check the operation of a computer system or computer data;

(c) to make and retain a copy of computer data;

(d) to remove computer data from a computer system or render the computer system inaccessible;

(e) to take a printout of computer data; or

(f) to impound or similarly secure a computer system or any part of the system.

(6) Any evidence seized under a Search and Seizure Warrant, including any computer system or data shall be valid for a period of ninety days and may, on an application to a Judge in Chambers, be extended for a further period of not more than one year.

(7) Upon the expiration of the period stated under sub-section (6), or when the evidence seized is no longer required, the evidence shall immediately be returned to the person to whom the Search and Seizure Warrant was addressed.

(8) Where a serious offence is being, has been or is likely to be committed for the benefit of, or at the direction of,

or in association with, a person, a group of persons or syndicate involved in organised crime or groups classified as criminal gangs, an application for a search and seizure warrant, shall not require the grounds under section 22(1)*(a)*.

(9) Where a Search and Seizure Warrant is based on the ground of national security, the application shall be accompanied by written authorisation by Minister.

Application for a Storage Direction or Search and Seizure Warrant.

22.–(1) A Court shall issue a Storage Direction or a Search and Seizure Warrant, where it is satisfied that the facts deponed there is reasonable grounds to believe that–

(a) obtaining the information sought is necessary in the interest of–

(i) national security;

(ii) public order;

(iii) public safety;

(iv) public health;

(v) preventing, detecting, investigating or prosecuting an offence under this Act or any other law; or

(vi) giving effect to the provisions of any mutual legal assistance request or in circumstances appearing to the Court to be equivalent to those in which he would issue a Storage Direction under sub-paragraph *(v)*; and

(b) other procedures–

(i) have not been or are unlikely to be successful in obtaining the information sought;

(ii) are too dangerous to adopt in the circumstances; or

(iii) are impractical having regard to the urgency of the case; or

(c) it would be in the best interest of the administration of justice to issue the Storage Direction.

(2) In considering an application under sub-section (1), the Court may require the applicant to furnish the Court with any further information as it deems necessary.

Extension of time for prosecution of an offence.

23. Notwithstanding the provisions of any written law prescribing the time within which proceedings for an offence punishable on summary conviction may be commenced, summary proceedings for an offence under this Act, or for attempting to commit, conspiring with another person to commit, or soliciting, inciting, aiding, abetting or counselling or causing or procuring the commission of, such an offence, or for attempting to solicit, incite, aid, abet, counsel or cause or procure the commission of such an offence, may be commenced within twelve months of the commission of the offence,

provided that where the offence is punishable on summary conviction and on conviction on indictment, nothing in this section shall be deemed to restrict the power to commence, after the expiry of the aforesaid period of twelve months, proceedings for conviction on indictment for that offence or for any other act, relating to the offence, referred to in this section.

Record of seized material.

24.–(1) A police officer who seizes or renders a computer system inaccessible under section 21, shall, at the time of the execution of the Search and Seizure Warrant, or as soon as practicable thereafter–

(a) make a list of the seized or rendered computer system, with the date and time of seizure or rendering; and

(b) submit a copy of the list to–

(i) the person to whom the warrant is addressed; or

(ii) the occupier of the premises at which the warrant is executed.

(2) A person, who immediately before the execution of a warrant, had possession or control of a computer system or a computer data storage medium seized, may request a copy of computer data from the police officer who executed the Search and Seizure Warrant, and the police officer shall, as soon as is reasonably practicable, comply with the request.

(3) Notwithstanding sub-section (2), a police officer who seizes a computer system or computer data storage medium may refuse to provide a copy of computer data if the police officer has reasonable grounds for believing that providing the copy would–

(a) constitute or facilitate the commission of a criminal offence; or

(b) prejudice–

(i) the investigation in relation to the Search and Seizure Warrant;

(ii) another ongoing investigation; or

(iii) any criminal proceedings that may be brought in relation to any investigation mentioned in sub-paragraph *(i)* or *(ii)*.

Assistance.

25.–(1) A person with knowledge about the functioning of a computer system or computer data storage medium, or security measures applied to protect computer data, that is the subject of a Search and Seizure Warrant shall, if requested, assist the police officer who is executing the search, by–

(a) providing any information, about the computer system, computer data or storage medium sought, that may facilitate the execution of the Search and Seizure Warrant;

(b) accessing and using the computer system or computer data storage medium to search computer data which is stored in, or lawfully accessible from or available to, that computer system or computer data storage medium;

(c) obtaining and copying computer data; or

(d) obtaining an intelligible output from a computer system or computer data storage medium in such a format that is admissible for the purpose of legal proceedings.

(2) A person who fails, without lawful excuse or justification, to comply with the requirements under sub-section (1), commits an offence and is liable on summary conviction to a fine of three thousand dollars and to a term of imprisonment for one year.

***Ex-parte* application for Production Order.**

26.–(1) The Director of Public Prosecutions or Head Prosecution Branch may, in the prescribed form, make an *ex-parte* application to the Court for a Production Order.

(2) An application under sub-section (1), shall be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following–

(a) the name of the investigating police officer;

(b) the facts or allegations giving rise to the application, including the alleged offence;

(c) full particulars of all facts and circumstances alleged by the applicant, including–

(i) where practical, a description of the nature and location of the facilities or computer from, or the premises at, which the application relates; and

(ii) the basis for believing that evidence relating to the ground on which the application is made will be obtained if the Production Order is granted;

(d) where applicable–

(i) whether other investigative procedures were applied and whether they failed to produce the required evidence; or

(ii) the reason why any other investigative procedures may be unlikely to succeed if applied, or are likely to be too dangerous to apply in order to obtain the required evidence;

(iii) the requested duration of the Order;

(iv) whether any previous application was made for a Production Order in respect of

the same person, facility or premises, and the status of that other application; and

(v) any other relevant directives issued by a Court in relation to the matter.

(3) A Court shall issue a Production Order, where it is satisfied that computer data or traffic data, a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings under this Act or any other law.

(4) A Production Order may direct–

(a) a person in Belize who is in possession or control of a computer system or computer data storage medium, to produce, from the computer system or computer data storage medium, specified computer data or a printout or other intelligible output of the computer data; or

(b) a service provider in Belize to produce traffic data relating to information transmitted from a subscriber through a computer system or from other relevant persons, or subscriber information about a person who uses the service, and give it to a specified person within a specified period.

Expedited Preservation Order.

27.–(1) A Judge, if satisfied on an *ex-parte* application by the Director of Public Prosecution, or a police officer of the rank of Superintendent or above that there are reasonable grounds to believe that computer data or traffic data that is reasonably required for the purpose of a criminal investigation, under this Act or any other law, is vulnerable to loss or modification, may make an order requiring a person in possession or control of computer data or traffic data to preserve and maintain the integrity of the computer data or traffic data for a period not exceeding ninety days.

(2) A Judge, on an *ex-parte* application by the Director of Public Prosecution or a police officer of the rank of Superintendent or above, may order an extension of the period referred to in subsection (1) by a further specified period of ninety days or more but not exceeding one year on a special case by case basis.

Removal or Disablement of Data Order.

28.–(1) The Director of Public Prosecutions or police officer, the rank of superintendent or above may, in the prescribed form, make an *ex-parte* application to the Court for a Removal or Disablement Order.

(2) Where on an application under sub-section (1), the Court is satisfied that a service provider or other entity within a domain name server is deleting, modifying, suppressing, storing, transmitting or providing access to computer data in contravention of this Act or any other law, the Court may order the service provider or entity to remove or disable access to the computer data.

Ex-parte application for Remote Forensic Tools Order.

29.–(1) The Director of Public Prosecutions may, in the prescribed form, make an *ex-parte* application to the Court for a Use of Remote Forensic Tools Order.

(2) An application under sub-section (1), shall be accompanied by an affidavit in support and attested to by the investigating police officer declaring the following–

(a) the basis for the application, including that it is the interest of–

(i) national security;

(ii) public safety;

(iii) public health;

(iv) public order;

(v) child luring or pornography;

(vi) human trafficking;

(vii) slavery; or

(viii) giving effect to the requirements of a mutual legal assistance request where the alleged offence is an offence under the laws of Belize.

(b) the name, and where possible, the address, of the person who is suspected of committing the alleged offence;

(c) a description of the targeted computer system;

(d) a description of the required tool, the extent and duration of its utilisation; and

(e) the reason for the use of the tool.

(3) A Court shall issue a Use of Remote Forensic Tools Order, where it is satisfied that computer data that is reasonably required for the purpose of a criminal investigation or criminal proceedings under this Act or any other law cannot be collected without the use of the Use of Remote Forensic Tools Order.

(4) On an application under subsection (1), the Court may order that a person or a service provider support the installation of the remote forensic tool.

(5) A Use of Remote Forensic Tools Order shall be in relation to the following only–

(a) modifications to a computer system shall be limited to those that are necessary for the investigation; and

(b) modification to a computer system shall be done, so far as possible, after the investigation.

(6) A police officer who executes a Use of Remote Forensic Tools Order as soon as possible after execution, prepare a record of–

(a) the remote forensic tool used;

(b) the time and date the remote forensic tool was used;

(c) the identification of the computer system and details of the modification undertaken; and

(d) the information obtained.

(7) A police officer who executes a Use of Remote Forensic Tools Order shall ensure that any information obtained by the utilisation of the remote forensic tool is protected against modification, unauthorised deletion and unauthorised access.

(8) A Use of Remote Forensic Tools Order shall cease to apply where–

(a) the computer data sought is collected;

(b) there is no longer any reasonable ground for believing that the computer data sought exists; or

(c) the conditions of the authorisation are no longer present.

(9) For the purposes of this section, "remote forensic tool" means an investigative software or hardware installed on or attached to a computer system that is used to perform a task.

Offence to disclose confidential information.

30.–(1) A person who is the subject of an Order under this Act shall not disclose to any other person–

(a) the fact that an Order was made;

(b) the details of the Order;

(c) anything done pursuant to the Order; or

(d) any compute or traffic data, subscriber information or other information collected or recorded pursuant to the Order under this Act.

(2) Sub-section (1) shall not apply to any actions between a service provider and any other person permitted under any law, or performed for the benefit of investigating or prosecuting an alleged offender.

(3) A person who without lawful excuse or justification, fails to comply with the requirements under sub-section (1), commits an offence and is liable on summary conviction to a fine of five thousand dollars and to a term of imprisonment for three years.

No liability for person aiding in enforcement of Act.

31. A person or service provider shall not be liable for any actions taken or the disclosure of any computer data or other information that may be disclosed pursuant to the enforcement of this Act.

Application for Compensation Order.

32.–(1) A person who believes that they have suffered loss or damage due to the commission of an offence under this Act, may make an application for a Compensation Order.

(2) The Court may make an order under sub-section (1) of its own motion.

(3) A Court shall, where it is satisfied on an application under sub-section (1), that the applicant has suffered pain and

suffering, loss, harm or injury, that is caused by the commission of an offence under this Act, grant the Compensation Order.

(4) A Compensation Order under sub-section (1) shall be without prejudice to any other remedy which the applicant has under any other law.

(5) An application under sub-section (1) shall be made prior to sentencing of the person against whom the Compensation Order is sought and be in accordance with rules of Court.

33.–(1) Subject to sub-section (2), where a person is convicted of an offence under this Act, the court that heard the criminal case may, upon the application of the Director of Public Prosecutions, order that any property–

***Ex-parte* application for Forfeiture Order and issue of Restraint Order.**

(a) used for or in connection with; or

(b) obtained as a result of or in connection with, the commission of the offence

be forfeited to the State.

(2) Before making a Forfeiture Order, the Court shall give an opportunity to be heard to any person who–

(a) claims to be the owner of the property that is the subject of the Order; or

(b) appears to the Court to have an interest in the property that is the subject of the Order.

(3) Where the Court is satisfied that the requirements under sub-section (2) have been met, the Court shall grant the Forfeiture Order and issue–

(a) a warrant authorising a police officer to search the building, place or vessel for the property

that is the subject of the Forfeiture Order and to seize–

(i) the property if found; and

(ii) any other property in respect of which the police officer has reasonable grounds to believe that the Forfeiture Order under ought to have been made; or

(b) a Restraint Order prohibiting any person from disposing of, or otherwise dealing with any interest in, the property, other than as specified in the Restraint Order.

(4) A person against whose property an Order under this section is made, may appeal the Order.

(5) Property forfeited to the State under sub-section (1) shall vest in the State–

(a) if no appeal is made against the Forfeiture Order, within the period for an appeal; or

(b) if an appeal is made, on the final determination of the matter, where the decision is made in favour of the State.

Failure to comply with a Court Order.

34. A person who fails to comply with any Order of the Court, under this Act, commits an offence and is liable–

(a) to a fine of one thousand dollars and to a term of imprisonment for one year; and

(b) where applicable, to a further daily fine for each day the offence continues, of not more than fifty thousand dollars until the relevant corrective action has been taken.

35. In any criminal proceedings under this Act or any other law– **Evidence.**

(a) any computer data or traffic data, generated, retrieved or reproduced from a computer system, and whether in electronic or printed form; or

(b) any computer acquired in respect of any offence,

shall be admissible as evidence.

36. It shall be within the discretion of the Director of Public Prosecutions to determine whether an offence is tried summarily or on indictment. **Determining the severity of charges.**

PART IV

International Cooperation

37. For the purposes of international cooperation, the Mutual Legal Assistance Act shall apply. **Mutual Legal Assistance Act No. 8 of 2014.**

38.–(1) The Central Authority may, concerning the possible commission of any offence under this Act, and without prior request, forward to foreign government or international agency information obtained within the framework of an investigation when it considers that the disclosure of the information might assist the foreign government or international agency in initiating or carrying out investigations or proceedings concerning criminal offences under its own law or applicable laws or might lead to a request for mutual legal assistance under this Act. **Spontaneous information.**

(2) The Central Authority may request that the information provided under sub-section (1) be kept confidential or only used subject to conditions.

(3) Where the information provided cannot kept confidential, the Central Authority may determine if the spontaneous information should be shared.

Extradition. CAP. 112.

39. The offences described in this Act shall be deemed to be extraditable offences and the Extradition Act shall apply.

Transborder access to computer data with consent or when unsecured and publicly available.

40. It shall not be an offence under this Act for any foreign government or any person to, without the authorisation of the Government of Belize or any person–

(a) access open source stored computer data, regardless of where the data is located, if the computer data is not subjected to security measures; or

(b) access or receive stored computer data located in Belize, if the foreign government or person obtains the consent of the person who has the authority to disclose the data through that computer system.

PART V

Miscellaneous

Use of computer system to commit offence under other law.

41. Where an offence, under any other law, is committed through the use of a computer system, the offender is liable on conviction to a fine of four times the penalty stated in the other law.

Corporate liability.

42.–(1) Where a body corporate commits an offence under this Act, the body corporate is liable to the fine applicable in respect of the offence.

(2) Where a body corporate commits an offence under this Act and the Court is satisfied that a director, manager, secretary, or other similar officer, of that body corporate–

(a) consented or connived in the commission of the offence; or

(b) failed to exercise due diligence to prevent the commission of the offence,

that director, manager, secretary, or other similar officer commits an offence.

(3) A person who commits an offence under sub-section (2) is liable on–

(a) summary conviction to a fine of ten thousand dollars and to imprisonment for three years; and

(b) on conviction on indictment to a fine of twenty thousand dollars and to imprisonment for five years.

Jurisdiction.

43. A Court in Belize shall have jurisdiction in respect of an offence under this Act where the act constituting the offence is carried out–

(a) wholly or in substantial part within its territory;

(b) against the status of persons, or interests in things, present within its territory;

(c) outside its territory but has or is intended to have substantial effect within its territory;

(d) against the activities, interests, status, or relations of its nationals outside as well as within its territory; and

(e) outside its territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests.

Regulations.

44. The Minister may make regulations prescribing all matters that are required to be prescribed under this Act and for such other matters as may be necessary for giving full effect to this Act and for its proper administration.

Printed in Belize by the Government Printer

Guidelines for Prosecuting Cases Involving Malicious Communications: Section 9 of the Cybercrimes Act of Jamaica, 2015

INTRODUCTION

These guidelines set out the approach that Prosecutors should take when making decisions in relation to cases where it is alleged that criminal offences have been committed by the sending of malicious communication via the use of a computer. They are designed to give clear guidance to Prosecutors who have been asked for early advice by the Police, and to guide the process when reviewing those cases which have been charged by the police.

These guidelines cover matters where a "computer" is used to send data (including images, messages) to another person, and where such data is menacing, threatening, or obscene. Therefore it is not limited to the sending of such communications via social media. In this guidance, we will explore the broad definition given to the word computer as contained within the **Cybercrimes Act, 2015**.

These guidelines are primarily concerned with offences that may be committed given the nature or content of the data sent via the use of a computer. Where the computer is used simply to facilitate some other substantive offence that may be charged and prosecuted under another Act or at common law, Prosecutors should first proceed under the substantive offence in question unless the situation lends itself convenient to prosecute an offence also under this Act. For example, if the Accused is charged with Demanding Money with Menaces contrary to **section 42A** of the **Larceny** Act but the demand was made by way of a computer, one may elect to proceed under the Larceny Act instead of **section 9** of the **Cybercrimes** Act. Experience has shown that as a Prosecutor one always strives for simplicity in laying charges for trial.

GENERAL PRINCIPLES

Prosecutors may only commence a prosecution if a case satisfies the test set out in **The Decision to Prosecute: A Jamaican Protocol. (Please see http:www.dpp.gov.jm.)** The test has two stages: the first is the requirement of evidential sufficiency and the second involves consideration of the public interest.

As far as the evidential stage is concerned, a Prosecutor must be satisfied that there is sufficient evidence to provide a realistic prospect of conviction. This means that an objective, impartial and reasonable jury (or Judge sitting alone), properly directed and acting in accordance with the law, is more likely than not to convict. It is an objective test based upon the Prosecutor's assessment of the evidence (including any information that he or she has about the defence).

A case which does not pass the evidential test MUST NOT PROCEED, regardless of how serious or sensitive it may be. In other words, if the material available on file does not cover the ingredients of the offence, then you cannot ethically proceed. Where the evidential test is achieved, the Prosecutor must go on to consider whether a prosecution is required in the public interest.

In the majority of cases, Prosecutors should only decide whether to prosecute after the investigation has been completed. However, there will be cases occasionally where it is clear, prior to the collection and consideration of all the likely evidence, that the public interest does not require a prosecution. In those cases, Prosecutors may decide that the case should not proceed further.

It is imperative and most useful that cases involving the sending of communications/ data via a computer undergo early consultation between Police and Prosecutors, and the Police are encouraged to contact the prosecution at an early stage of the investigation.

WHAT IS A COMPUTER?

A computer is defined in **Section 2** of the **Cybercrimes** Act as any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs the automatic processing of data. It also includes a data storage facility, or electronic communication system. An electronic communication system is further defined as any system for creating, sending, receiving, storing, displaying, or processing electronic data. This definition is wide enough to capture such devices as thumb drives, smart phones, IPads, and tablets.

OFFENCE: USE OF A COMPUTER FOR MALICIOUS COMMUNICATION, SECTION 9 CYBERCRIMES ACT

There are three ingredients that must be proved by the material presented to an Investigator before a prosecution can be initiated under this section. They are:

1. That a person used a computer to send to another person data.

   Send is not defined under any current legislation and as such arguably it may include the publishing of material by a person to a social media site.

2. That the data sent is **obscene or constitutes a threat or is menacing in nature.** These terms are also not defined by the legislation.

   Material that is obscene is of a sexual nature or offends against society's morality and tends to deprave or corrupt minds open to immoral influences and into whose hands these publications would fall.

   Threatening material is material that intimates that harm/danger/punishment will befall a person and may be similar to a menace.

   Material that is menacing in nature tends to threaten with harm or danger.

3. ***AND***, that the material which is either obscene or a threat or menacing in nature, or all three, or a combination of the three, was sent ***with the intention*** to harass any person or cause harm or the apprehension of harm, to any person or property.

Intention may be proved by direct evidence such as statements of the suspect showing their intention or it may be inferred from all the circumstances.

These three elements referred to above must all exist in order for a section 9 offence to be created. It is also clear from this section that there is no requirement for the material published to be false or cause harm to a person's reputation and the like and as such fall under the heading of defamation. A section 9 offence may exist even where a statement is true which takes it outside the tort of defamation.

CATEGORY 1. THE TRANSMISSION OF DATA WHICH IS OBSCENE.

Communications via a computer which are obscene can be considered under the Obscene **Publications Act** or the **Cybercrimes Act, 2015**. In the year 1927, the **Obscene Publications (Suppression) Act** was passed. This Act created the offences of Possession, Distribution and Publication of obscene writings, drawings, and photographs etc. The penalty if convicted remains at the paltry sum of Jamaican $40.00. Before the passage of the 2015 **Cybercrimes Act**, the publication or distribution of obscene images on the internet, or otherwise would give rise to a penalty of $40.00.

WHAT IS OBSCENE DATA?

Obscene is not defined by the **Cybercrimes Act**. The definition of obscenity stated by Cockburn C.J in ***R v Hicklin (1868) L.R. 3 Q.B. 360*** was:

> *"the test of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall."*

The present common law meaning of obscene is to be found in the case of ***R v. Anderson (1971) 3 W.L.R. 939***. It was stated therein that obscene is not confined to sexual content. The word obscene is not defined in the **Obscene Publications Act of Jamaica**. As such the common law definition is applicable. The words "indecent" and "obscene" convey the idea of offending against property, indecency being at the lower, and obscenity at the upper end of the scale. An indecent article is not necessarily obscene, but an obscene article is most certainly indecent. ***R v Stanley (1965) 2 Q.B. 32***.

CATEGORIES 2 AND 3. DATA THAT IS THREATENING AND DATA THAT IS MENACING IN NATURE

THREATS

Communications which may constitute threats of violence to the person or property may constitute a number of offences, including those set out below.

A threat to kill contrary to **section 18** of the ***Offences against the Person Act Jamaica*** can be considered where the communication constitutes a direct threat to kill. This section reads:

> *"Whosoever shall maliciously send, deliver, or utter, or directly or indirectly cause to be received, knowing the contents thereof, any letter or writing threatening to kill or murder any person, shall be guilty of a felony, and being convicted thereof, shall be liable to be imprisoned for a term not exceeding ten years, with or without hard labour."*

Where the prosecution seeks to advance a case under **section 18** of the ***Offences Against the Person Act***, there must be evidence that the accused sent or delivered the writing to the complainant, and further it is a question of fact for the jury whether the contents of the writing amounts to a threat to kill or murder ***R v Boucher***, *4 C &P. 562; R v Tyler, 1 Mood. 428. Cited in* ***Archbold Pleading, Evidence & Practise in Criminal Cases 36th Edition at p.3615.***

Threats of violence to the person or damage to property may also fall to be considered under section 9 of the ***Cybercrimes Act, 2015***.

MENACES

This section prohibits the sending of data which is threatening or menacing in nature. The **Cybercrimes Act** does not define the term menace, and as such the common law definition will be applicable in the interpretation of the statute.

However, where the prosecution is seeking to prove that the message is of a menacing nature, before proceeding with such a prosecution, Prosecutors should heed the words of the Lord Chief Justice in ***Chambers v DPP [2012] EWHC 2157 (Admin)*** paragraph 30 where he said:

> *"… a message which does not create fear or apprehension in those to whom it is communicated, or may reasonably be expected to see it, falls outside,… for the simple reason that the message lacks menace."*

The case of ***Chambers v DPP*** also cited Sedley LJ in ***DPP v Collins [2006] 1WLR 308*** where he stated in the context of a message which was menacing that:

> *"…fairly plainly, is a message which conveys a threat – in other words, which seeks to create a fear in or through the recipient, that something unpleasant is going to happen…"*

THE HIGH THRESHOLD AT THE EVIDENTIAL STAGE

There is a high threshold that must be met before the evidential stage in the **The Decision to Prosecute: A Jamaican Protocol** will be satisfied.

Prosecutors ought to bear in mind that what is prohibited under **section 9** of the **Cybercrimes Act 2015** is the sending of data which is threatening, menacing or obscene. Therefore a communication that is sent has to be more than simply offensive to be contrary to the criminal law. Just because the content expressed in the communication is offensive, done in bad taste, controversial or unpopular, or defamatory, this is not a sufficient reason to engage the criminal law. The comment of the Lord Chief Justice in the case of ***Chambers v DPP [2012] EWHC 2157 (Admin)*** is applicable to our legislative context. He stated, in relation to section 127 of the **Communications Act 2003 UK** which prohibited communication that was grossly offensive, as follows;

> "*Satirical, or iconoclastic, or rude comment, the expression of unpopular or unfashionable opinion about serious or trivial matters, banter or humour, even if distasteful to some or painful to those subjected to it should and no doubt will continue*

at their customary level, quite undiminished by [section 127 of the **Communications Act 2003 UK***]".*

In Jamaica's legislative context, **section 9** is specific in that it prohibits obscene communication, and therefore it is not concerned with whether the communication is offensive, but whether it has a tendency to deprave and corrupt.

CONTEXT AND APPROACH: THE MENTAL ELEMENT (MENS REA)

Prosecutors must bear in mind that before a decision is taken to prosecute, the context in which the communication is sent is of utmost importance in determining whether there exists evidence of a criminal intent to harass any person or cause harm or the apprehension of harm, to any person or property. The **Cybercrimes Act** requires proof of an intention to cause harm or the apprehension of harm and this is the highest level of subjective mens rea.

Recklessness or negligence concerning whether the sending of the information would cause harm is insufficient. This is a critical consideration before a decision to prosecute is made. In the context of social media where communication may be sent as banter, jokes, or even careless commentary, there must be evidence of a criminal intent. Therefore due regard will have to be given to the surrounding circumstances in which the message or data was sent to satisfy this element of the offence.

THE PUBLIC INTEREST STAGE

When the Prosecutor is satisfied that the evidential criteria is met, a prosecution will usually take place unless the Prosecutor concludes that there are public interest factors tending against prosecution which outweigh those tending in favour. Prosecutors must be guided by **The Decision to Prosecute: A Jamaican Protocol (http:www.dpp.gov.jm**) which contains the public interest test that informs the decision to prosecute.

CONSEQUENCES OF FAILING TO FOLLOW THE GUIDELINES

Prosecutors and Law Enforcement should be mindful that communications via computers and in particular via the use of social media is so vast in the 21st century that it cannot be quantified. It is truly global and without any borders – at the click of a button. Without adhering to these guidelines Law Enforcement, the Prosecuting authority and possibly members of the public who are potential complainants, could run the risk of placing a large number of cases in the Court arena which at first blush may pass the public interest test but when closely examined within the context of the guidelines would not pass the evidential test and therefore would not form the basis of a viable case to prosecute. It behoves all of us to remember that the process of assessing whether a matter should be prosecuted cannot be viewed back ways; that is from public interest to the evidential test. It must be emphasized that the evidential test as previously described ***MUST*** be passed before one considers the public interest test.

There is no room for emotion or anything else that is extraneous to the considerations previously outlined. ***That is the ethical imperative under which prosecutions are bound to take place*.** Always remembering that the burden of proving the case beyond a reasonable doubt in Court rests on the shoulders of the prosecution and it never shifts. The ultimate consequence of placing a matter before the Criminal Court that does not satisfy the evidential test will mean that a case will be thrown out.

I trust that by prescribing these guidelines it will assist in transparency and the understanding by Prosecutors, Law Enforcement and Members of the Public in the use of section 9 of the Cybercrimes Act, 2015.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
Clause 4	Illegal access	Conviction on indictment: A fine of $50 000 or to imprisonment for a term of 5 years or to both.	Section 4	Conviction on indictment: A fine of $25 000 or imprisonment for a term of 2 years or to both.	Section 3	Summary conviction: 1st offence - a fine not exceeding $3 million JMD ($39 101.67 BBD) or to imprisonment for a term not exceeding 3 years; **OR** If any damage is caused as a result of the commission of the offence, a fine not exceeding $4 million JMD ($51 996.25 BBD) or to imprisonment for a term not exceeding 4 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine not exceeding $5 million JMD ($65 169.44 BBD) or to imprisonment for a term not exceeding 5 years; **OR**	Section 3	Summary conviction: A fine of $3 million GYD ($29 012.18 BBD) and to imprisonment for a term of 3 years; **OR** Conviction on indictment: A 5 million GYD ($48 353.63 BBD) and to imprisonment for a term of 5 years.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
						Conviction on indictment: 1st offence - a fine or imprisonment for a term not exceeding 7 years; **OR** If any damage is caused as a result of the commission of the offence, a fine or to imprisonment for a term not exceeding 10 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine or to imprisonment for a term not exceeding 15 years.		
Clause 5	Modification of programme or data	Conviction on indictment: A fine of $70 000 or to imprisonment for a term of 7 years or to both.	N/A New offence	N/A New offence	Section 5(3)	Summary conviction: 1st offence - a fine not exceeding $3 million JMD ($39 101.67 BBD) or to imprisonment for a term not exceeding 3 years; **OR**	N/A	N/A

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
						If any damage is caused as a result of the commission of the offence, a fine not exceeding $4 million JMD ($51 996.25 BBD) or to imprisonment for a term not exceeding 4 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine not exceeding $5 million JMD ($65 169.44 BBD) or to imprisonment for a term not exceeding 5 years; **OR** Conviction on indictment: 1st offence - a fine or imprisonment for a term not exceeding 7 years; **OR** If any damage is caused as a result of the commission of the offence,		

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
						a fine or to imprisonment for a term not exceeding 10 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine or to imprisonment for a term not exceeding 15 years.		
Clause 6	Interfering with programme or data	Conviction on indictment: A fine of $70 000 or to imprisonment for a term of 7 years or to both.	Section 5 Interfering with data	Conviction on indictment: A fine of $50 000 or to imprisonment for a term of 5 years or to both.	N/A	N/A	Section 5(2)(b)	Summary conviction: A fine of $3 million GYD ($29 012.18 BBD) and to imprisonment for a term of 3 years; **OR** Conviction on indictment: A fine of $8 million GYD ($77 365.80 BBD) and to imprisonment for a term of 5 years.
Clause 7	Interfering with computer system	Conviction on indictment: A fine of $70 000 or to imprisonment for a term of 7 years or to both.	Section 6	Conviction on indictment: A fine of $50 000 or to imprisonment for a term of 5 years or to both.	N/A	N/A	Section 7(2)(b)	Summary conviction: A fine of $3 million GYD ($29 012.18 BBD) and to imprisonment for a term of 3 years; **OR** Conviction on indictment: 8 million GYD ($77 365.80 BBD) and to imprisonment for a term of 5 years.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
Clause 8	Illegal interception of data	Conviction on indictment: A fine of $100 000 or to imprisonment for a term of 10 years or to both.	Section 7	Conviction on indictment: A fine of $50 000 or to imprisonment for a term of 5 years or to both.	Section 6(5)(a)	Summary conviction: 1st offence - a fine not exceeding $3 million JMD ($39 101.67 BBD) or to imprisonment for a term not exceeding 3 years; **OR** If any damage is caused as a result of the commission of the offence, a fine not exceeding $4 million JMD ($51 996.25 BBD) or to imprisonment for a term not exceeding 4 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine not exceeding $5 million JMD ($65 169.44 BBD) or to imprisonment for a term not exceeding 5 years; **OR** Conviction on indictment:	Section 4(3)	Summary conviction: A fine of $5 million GYD ($48 353.63 BBD) and to imprisonment for a term of 3 years; **OR** Conviction on indictment: 8 million GYD ($77 365.80 BBD) and to imprisonment for a term of 5 years.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
						1st offence - a fine or imprisonment for a term not exceeding 7 years; **OR** If any damage is caused as a result of the commission of the offence, a fine or to imprisonment for a term not exceeding 10 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine or to imprisonment for a term not exceeding 15 years.		
Clause 9	Illegal devices	Conviction on indictment: A fine of $70 000 or to imprisonment for a term of 7 years or to both.	Section 8	Conviction on indictment: A fine of $50 000 or to imprisonment for a term of 5 years or to both.	N/A	N/A	Section 8(2)	Summary conviction: A fine of $3 million GYD ($29 012.18 BBD) and to imprisonment for a term of 3 years; **OR** Conviction on indictment: 8 million GYD ($77 365.80 BBD) and to imprisonment for a term of 5 years.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
Clause 10	Access with intent to commit further offence	Conviction on indictment: A fine of $70 000 or to imprisonment for a term of 7 years or to both.	Section 9	Conviction on indictment: A fine of $50 000 or to imprisonment for a term of 5 years or to both.	Section 10 (2)	Summary conviction: 1st offence - a fine not exceeding $4 million JMD ($52 135.56 BBD) or to imprisonment for a term not exceeding 4 years; **OR** If any damage is caused as a result of the commission of the offence, a fine not exceeding $5 million JMD ($65 169.44 BBD) or to imprisonment for a term not exceeding 5 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine not exceeding $5 million JMD ($65 169.44 BBD) or to imprisonment for a term not exceeding 5 years; **OR** Conviction on indictment:	Section 23	Four times the monetary value provided by that law and the same custodial sentence

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
						1st offence - a fine or imprisonment for a term not exceeding 10 years; **OR** If any damage is caused as a result of the commission of the offence, a fine or to imprisonment for a term not exceeding 15 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine or to imprisonment for a term not exceeding 20 years.		
Clause 11	Disclosure of access code	Summary conviction: A fine of $25 000 or to imprisonment for a term of 3 years or to both.	Section 10	Summary conviction: A fine of $10 000 or to imprisonment for a term of 12 months or to both and, in the case of a second or subsequent	N/A	N/A	Section 9(1)	Summary conviction: A fine of $3 million GYD ($29 012.18 BBD) and to imprisonment for a term of 3 years; **OR** Conviction on indictment: 8 million GYD ($77 365.80 BBD) and to imprisonment for a term of 5 years.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
		Conviction on indictment: A fine of $70 000 or to imprisonment for a term of 7 years or to both.		conviction, to a fine of $20 000 or to imprisonment for a term of 2 years or to both Conviction on indictment: A fine of $50 000 or to imprisonment for a term of 5 years or to both and, in the case of a second or subsequent conviction, to a fine of $100 000 or to imprisonment for a term of 7 years or to both				
Clause 12	Critical information infrastructure system	A person who without authority, gains access or interferes with –	N/A	N/A	N/A	N/A	Section 12(1)	Conviction on indictment: 20 million GYD ($193 414.50 BBD) and to imprisonment for a term of 10 years.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
		Conviction on indictment: A fine of $100 000 or to imprisonment for a term of 10 years or to both. In the course of commission of any offence – Conviction on indictment: A fine of $150 000 or to imprisonment for a term of 12 years or to both						
Clause 13	Receiving or giving of access to computer programme or data	Conviction on indictment: A fine of $70 000 or to imprisonment for a term of 7	Section 12	Conviction on indictment: A fine of $50 000 or to imprisonment for a term of 5	N/A	N/A	Section 9(2)(b)	Summary conviction: A fine of $3 million GYD ($29 012.18 BBD) and to imprisonment for a term of 3 years; **OR**

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
		years or to both.		years or to both				Conviction on indictment: 8 million GYD ($77 365.80 BBD) and to imprisonment for a term of 5 years.
Clause 14	Computer-related forgery	Conviction on indictment: A fine of $100 000 or to imprisonment for a term of 10 years or to both.	N/A New offence	N/A New offence	Section 8 (2)	Summary conviction: 1st offence - a fine not exceeding $4 million JMD ($52 135.56 BBD) or to imprisonment for a term not exceeding 4 years; **OR** If any damage is caused as a result of the commission of the offence, a fine not exceeding $5 million JMD ($65 169.44 BBD) or to imprisonment for a term not exceeding 5 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine not exceeding $5 million JMD ($65 169.44 BBD) or to imprisonment for a	Section 10	Summary conviction: A fine of $3 million GYD ($48 353.63 BBD) and to imprisonment for a term of 3 years; **OR** Conviction on indictment: 5 million GYD ($77 365.80 BBD) and to imprisonment for a term of 5 years.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
						term not exceeding 5 years; **OR** Conviction on indictment: 1st offence - a fine or imprisonment for a term not exceeding 10 years; **OR** If any damage is caused as a result of the commission of the offence, a fine or to imprisonment for a term not exceeding 15 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine or to imprisonment for a term not exceeding 20 years.		
Clause 15	Computer-related fraud	Conviction on indictment: A fine of $100 000 or to	N/A New offence	N/A New offence	Section 8 (2)	Summary conviction: 1st offence - a fine not exceeding $4 million JMD ($52 135.56 BBD) or to	Section 11(2)	Summary conviction: 5 million GYD ($77 365.80 BBD) and to imprisonment for a term of 5 years; **OR**

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
		imprisonment for a term of 10 years or to both.				imprisonment for a term not exceeding 4 years; **OR** If any damage is caused as a result of the commission of the offence, a fine not exceeding $5 million JMD ($65 169.44 BBD) or to imprisonment for a term not exceeding 5 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine not exceeding $5 million JMD ($65 169.44 BBD) or to imprisonment for a term not exceeding 5 years; **OR** Conviction on indictment: 1st offence - a fine or imprisonment for a term not exceeding 10 years; **OR**		Conviction on indictment: 10 million GYD ($96 707.25 BBD) and to imprisonment for a term of 10 years.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
						If any damage is caused as a result of the commission of the offence, a fine or to imprisonment for a term not exceeding 15 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine or to imprisonment for a term not exceeding 20 years.		
Clause 16	Child pornography	Conviction on indictment: In the case of an individual, to a fine of $100 000 or to imprisonment for a term of 10 years or both; or In the case of a corporation,	Section 13	Conviction on indictment: In the case of an individual, to a fine of $50 000 or to imprisonment for a term of 5 years or both; or In the case of a corporation, to a fine of $200 000.	N/A	N/A	Section 14(4)(b)	Summary conviction: 10 million GYD ($96 707.25 BBD) and to imprisonment for a term of 5 years; **OR** Conviction on indictment: 15 million GYD ($145 060.88) and to imprisonment for a term of 10 years.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
		to a fine of $250 000.						
Clause 17	Child grooming	Conviction on indictment: In the case of an individual, to a fine of $100 000 or to imprisonment for a term of 10 years or both; or In the case of a corporation, to a fine of $250 000.	N/A New offence	N/A New offence	N/A	N/A	Section 15(4)	Summary conviction: A fine of $3 million GYD ($29 012.18 BBD) and to imprisonment for a term of 5 years; **OR** Conviction on indictment: 8 million GYD ($77 365.80 BBD) and to imprisonment for a term of 5 years.
Clause 18	Online child sexual abuse	Conviction on indictment: In the case of an individual, to a fine of $100 000 or to imprisonment for a term of	N/A New offence	N/A New offence	N/A	N/A	N/A	N/A

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
		10 years or both; or In the case of a corporation, to a fine of $250 000.						
Section 19	Malicious communications	Summary conviction: A fine of $70 000 or to imprisonment for a term of 7 years or to both.	Section 14	Summary conviction: A fine of $10 000 or to imprisonment for a term of 12 months or to both.	Section 9(3)	Summary conviction: 1st offence - a fine not exceeding $4 million JMD ($52 135.56 BBD) or to imprisonment for a term not exceeding 4 years; **OR** If any damage is caused as a result of the commission of the offence, a fine not exceeding $5 million JMD ($65 169.44 BBD) or to imprisonment for a term not exceeding 5 years; **OR** In the case of a 2nd or subsequent offence, regardless of if any damage is caused, a fine not exceeding	Section 19(5)	Summary conviction: A fine of $5 million GYD ($48 353.63 BBD) and to imprisonment for a term of 3 years; **OR** Conviction on indictment: 10 million GYD ($96 707.25 BBD) and to imprisonment for a term of 5 years.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
						$5 million JMD ($65 169.44 BBD) or to imprisonment for a term not exceeding 5 years; **OR** Conviction on indictment: 1st offence - a fine or imprisonment for a term not exceeding 10 years; **OR** If any damage is caused as a result of the commission of the offence, a fine or to imprisonment for a term not exceeding 15 years; **OR** In the case of a 2nd or subsequent offence, regardless of it any damage is caused, a fine or to imprisonment for a term not exceeding 20 years.		

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
Clause 20	Cyber bullying	Summary conviction: A fine of $70 000 or to imprisonment for a term of 7 years or to both.	N/A New offence	N/A New offence	N/A	N/A	N/A	N/A
Clause 21	Cyber terrorism	Conviction on indictment: Imprisonmet for a term of 25 years.	N/A New offence	N/A New offence	N/A	N/A	N/A	N/A
Clause 22	Aiding or abetting	A person who aids or abets the commission of an offence under this Act is guilty of that offence and is liable to the penalty of that offence.	N/A New offence	N/A New offence	N/A	N/A	Section 22 Attempt, aiding or abetting	Shall be punished for the offence as if he had committed the offence as a principal offender.

Cybercrime Bill	Offence	Penalty	Computer Misuse Act, Cap. 124B	Penalty	Jamaica – Cybercrimes Act, 2015	Penalty	Guyana – Cybercrime Act, 2018	Penalty
Clause 23(5)	Search and seizure	A person who obstructs a police officer… Summary conviction: A fine of $25 000 or to imprisonment for a term of 2 years or to both.	Section 15(4)	A person who obstructs a police officer… Summary conviction: A fine of $15 000 or to imprisonment for a term of 18 months or to both.	N/A	N/A	N/A	N/A
Clause 24 (3)	Failure to assist a police officer	Summary conviction: A fine of $25 000 or to imprisonment for a term of 2 years or to both.	Section 16(2)	Summary conviction: A fine of $15 000 or to imprisonment for a term of 18 months or to both.	N/A	N/A	Section 30(2)	Summary conviction: A fine of $3 million GYD ($29 012.18 BBD) and to imprisonment for a term of 1 years.

NEW BILL

2024-07-12

OBJECTS AND REASONS

This Bill would provide for

(a) the combatting of cybercrime;

(b) the protection of legitimate interests in the use and development of information technologies;

(c) the facilitation of international co-operation in computer related crimes;

(d) the repeal of the *Computer Misuse Act*, Cap. 124B; and

(e) related matters.

Arrangement of Sections

PART I

PRELIMINARY

PART II

PROHIBITED CONDUCT

BARBADOS

A Bill entitled

An Act to provide for the combatting of cybercrime, protection of legitimate interests in the use and development of information technologies, the facilitation of international co-operation in computer related crimes and related matters.

ENACTED by the Parliament of Barbados as follows:

PART I

PRELIMINARY

Short title

1. This Act may be cited as the *Cybercrime Act, 2024.*

Interpretation

2.(1) In this Act,

"approved person" means a person who has the relevant training and skill in computer systems and technology, who has knowledge about the functioning of the computer system and is identified, in writing, by the Commissioner of Police or other gazetted officer designated by the Commissioner, to assist the police;

"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function;

"computer data storage medium" means any article or material from which electronic information is capable of being reproduced, with or without the aid of any other electronic article or device;

"computer programme" or "programme" means data or a portion of data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;

"computer system" means a device or a group of inter-connected or related devices, one or more of which, pursuant to a programme, facilitates communication, performs automatic processing of data or any other function;

"**cyber bullying**"**means the behaviour or conduct referred to at section 20;**

"damage" includes

(a) any impairment to the integrity of a computer system or the integrity or availability of any data or programme held in a computer system; and

(b) the impairment of the confidentiality of data or programme held in a computer system;

"intercept" includes, in relation to a computer system, listening to, monitoring or surveillance of or recording a function of a computer system, or acquiring the substance, meaning or purport of the function;

"service provider" means

(a) a public or private entity that provides to users of its services the ability to communicate by means of a computer system; and

(b) any other entity that processes or stores computer data on behalf of that entity or its users;

"ship" means a vessel which is designed, used or capable of being used solely or partly for navigation in, on, through, or immediately above the water, without regard to method or lack of propulsion and includes a maritime autonomous surface ship;

"traffic data" means computer data that

(a) relates to a communication by means of a computer system;

(b) is generated by a computer system that is part of a chain of communication; and

(c) shows the origin, destination, route, time, date, size, duration of the communication or the type of underlying services;

"**without authority**"**means without right, consent, permission, authorization or in excess of authorization.**

(2) For the purposes of this Act, access of any kind by a person to any computer system, programme or data is obtained without authority if he knows that he is not entitled to access of the kind in question relating to the computer system, programme or data and

(a) he accesses the computer system, programme or data; or

(b) he exceeds any right or permission to access the computer system, programme or data from any person who may permit such access.

(3) A reference in this Act to any "programme or data" held in a computer system includes a reference to

(a) any programme or data held in any removable storage medium which is for the time being in the computer system; or

(b) any programme or data held in any storage medium which is external to the computer system, but which is connected to it.

(4) For the purposes of this Act, a modification of the contents of any computer system takes place if, by the operation of any function of the computer system concerned or of any other computer system

(a) any programme or data held in the computer system is altered or erased;

(b) any programme or data is added to any programme or data held in the computer system; or

(c) any act occurs which impairs the normal operation of any computer system,

and any act which contributes towards such a modification shall be regarded as causing it.

(5) Any modification referred to in subsection (4) is without authority if the person whose act causes the modification

(a) knows that he is not entitled to determine whether the modification should be made; and

(b) has not obtained the consent of the person who is entitled to consent to the modification.

(6) A reference in this Act to a programme includes a reference to a part of a programme.

Application

3.(1) This Act applies to an act done or an omission made

(a) in Barbados;

(b) on a ship or aircraft registered in Barbados; or

(c) by a national of Barbados outside the territory of Barbados, if the person's conduct would also constitute an offence under the law of a country where the offence was committed.

(2) For the purpose of paragraph *(a)* of subsection (1), an act is carried out in Barbados if

(a) the person is in Barbados when the act is committed; or

(b) the person is outside Barbados at the time when the act is committed but

(i) a computer system located in Barbados or electronic data storage medium located in Barbados is affected by, or contains information about the act; or

(ii) transmission or effect of the act, or the damage resulting from the act, occurs in whole or in part within Barbados.

(3) The *Mutual Assistance in Criminal Matters Act*, Cap. 140A shall apply to this Act in relation to an offence under this Act as if the offence were a serious offence within the meaning of section 2 of that Act.

PART II

PROHIBITED CONDUCT

Illegal access

4.(1) A person who intentionally or recklessly and without authority,

(a) gains access to the whole or any part of a computer system;

(b) causes a programme to be executed; or

(c) uses a programme to gain access to any data,

is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

(2) For the purposes of subsection (1), the form in which any programme or data is accessed or obtained and, in particular, whether or not it represents a form in which it is capable of being executed is immaterial.

Modification of programme or data

5.(1) A person who intentionally or recklessly and without authority causes any modification to a programme or data is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) For the purposes of subsection (1), the act in question need not be directed at

(a) any specifically identifiable programme or data or type of programme or data; or

(b) any programme or data that is held in a specifically identifiable computer system.

(3) For the purposes of subsection (1), it is immaterial whether the modification is or is intended to be permanent or temporary.

Interfering with programme or data

6.(1) A person who intentionally or recklessly and without authority,

(a) copies or moves a programme or data

(i) to any storage medium other than that in which that programme or data is held; or

(ii) to a different location in the storage medium in which that programme or data is held;

(b) destroys or erases a programme or data;

(c) damages a programme or data;

(d) suppress a programme or data;

(e) adds, deletes or alters a programme or data;

(f) renders a programme or data meaningless, useless or ineffective;

(g) obstructs, interrupts or interferes with the lawful use of a programme or data; or

(h) denies access to a programme or data,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) Subsection (1) applies whether the person's act is of temporary or permanent effect.

(3) For the purposes of subsection (1), the form in which a programme or data is copied and, in particular, whether or not it represents a form in which it is capable of being executed is immaterial.

Interfering with computer system

7. A person who intentionally or recklessly and without authority,

(a) hinders the functioning of a computer system by

(i) causing electromagnetic interference to a computer system;

(ii) accessing or causing access to a computer system; or

(iii) corrupting a computer system by any means; or

(b) interferes with the functioning of a computer system,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Illegal interception of data

8. A person who intentionally and without authority, undertakes an act to intercept by technical means any non-public transmission to, from or within a computer system, including electromagnetic emissions from a computer system carrying computer data, is guilty of an offence and is liable on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

Misuse of devices

9. A person who intentionally or recklessly and without authority,

(a) produces, sells, procures for use, imports, exports, distributes or otherwise makes available

(i) a device, including a computer programme, that is primarily designed or adapted for the purpose of committing an offence; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being

accessed, with the intent that it be used by any person for the purpose of committing an offence; or

(b) has an item mentioned in paragraph (*a*)(i) or (ii) in his possession with the intent that it be used by himself or any other person for the purpose of committing an offence,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Access with intent to commit further offence

10. A person who intentionally and without authority uses a computer system to perform any function in order to secure access to any programme or data held in that computer system or in any other computer system with the intention to commit a further offence is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Disclosure of access code

11.(1) A person who intentionally or recklessly and without authority discloses any password, access code or any other means of gaining access to any programme or data held in a computer system is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 3 years or to both.

(2) A person who intentionally or recklessly and without authority discloses any password, access code or any other means of gaining access to any programme or data held in a computer system for any unlawful gain, whether to himself or to another person, knowing that it is likely to cause unlawful damage, is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

Critical information infrastructure system

12.(1) For the purposes of this section "critical information infrastructure system" means any computer system, programme or data that supports or performs a function that relates to

(a) electricity generation or distribution**;**

(b) telecommunications;

(c) government services;

(d) emergency services;

(e) law enforcement, security or intelligence agencies;

(f) public works; or

(g) any computer system, programme or data that may be designated as a critical information infrastructure system by the Minister responsible for the prevention of cybercrime, published in the *Official Gazette*,

that is so vital that the incapacity or destruction of such computer system, programme or data would have a debilitating impact on the security, national economic security, national public health or safety or any combination of those matters, in Barbados.

(2) A person who without authority,

(a) gains access to; or

(b) interferes with

a critical information infrastructure system is guilty of an offence and is liable on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

(3) A person who without authority gains access to or interferes with a critical information infrastructure system in the course of the commission of any offence

is liable on conviction on indictment to a fine of $150 000 or to imprisonment for a term of 12 years or to both.

(4) It shall be a defence to a charge brought under subsection (2) or (3) to prove that access to or interference with a critical information infrastructure system was obtained inadvertently and with no intent to commit an offence.

Receiving or giving of access to computer programme or data

13.(1) A person who

(a) intentionally or recklessly and without authority receives or is given access to any programme or data; and

(b) knows or believes that

(i) the programme or data was obtained without authority; or

(ii) access to the programme or data was obtained without authority,

is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of 7 years or to both.

(2) It shall be a defence to a charge brought under subsection (1) to prove that the programme or data or access to the programme or data

(a) was received inadvertently and with no intent to commit an offence;

(b) was subject to legal privilege; **or**

(c) was received by a law enforcement officer in the course of an investigation.

Computer-related forgery

14. A person who intentionally and without authority, inputs, alters, deletes or suppresses a programme or data that results in inauthentic data being considered or acted on for any legal purpose as if it were authentic, whether or not the data is directly readable and intelligible, is guilty of an offence and liable

on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

Computer-related fraud

15. A person who intentionally, fraudulently or dishonestly and without authority, inputs, alters, deletes or suppresses any computer data or interferes with the functioning of a computer system for the purpose of

(a) procuring an economic benefit for himself or another person;

(b) causing loss of property to a person;

is guilty of an offence and is liable on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.

Child pornography

16.(1) A person who intentionally or recklessly

(a) publishes child pornography through a computer system;

(b) produces child pornography for the purpose of its publication through a computer system;

(c) possesses child pornography in a computer system or on a computer data storage medium for the purpose of publication; or

(d) procures child pornography through a computer system for himself or for another person,

is guilty of an offence and is liable on conviction on indictment,

(i) in the case of an individual, to a fine of $100 000 or to imprisonment for a term of 10 years or to both; or

(ii) in the case of a corporation, to a fine of $250 000.

(2) It shall be a defence to a charge brought under subsection (1) if the person establishes that the child pornography was for a *bona fide* research, medical or law enforcement purpose.

(3) For the purposes of subsection (1),

(a) “child” means a person under the age of 18 years;

(b) "child pornography" includes material that visually depicts

(i) a child engaged in sexually explicit conduct;

(ii) a person who appears to be a child engaged in sexually explicit conduct; or

(iii) realistic images representing a child engaged in sexually explicit conduct; and

(c) "publish" includes

(i) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way;

(ii) have in possession or custody, or under control, for the purpose of doing an act referred to in paragraph *(b)*; or

(iii) print, photograph, copy or make in any other manner, whether of the same or of a different kind or nature, for the purpose of doing an act referred to in paragraph *(b)*.

Child grooming

17. A person who intentionally or recklessly uses a computer system to befriend, manipulate, communicate with or establish a connection with a child in order to abuse the child, whether sexually or otherwise, is guilty of an offence and is liable on conviction on indictment

(a) in the case of an individual to a fine of $100 000 or to imprisonment for a term of 10 years or to both; or

(b) in the case of a corporation, to a fine of $250 000.

Online child sexual abuse

18.(1) A person who intentionally or recklessly uses a computer system to meet a child for the purpose of

(a) engaging in sexual activity with a child;

(b) engaging in sexual activity with the child where

(i) coercion, inducement, force or threat is used;

(ii) a recognised position of trust, authority or influence over the child, including within the family is abused; or

(iii) a child's mental or physical disability or situation of dependence is abused

is guilty of an offence.

(2) A person who is guilty of an offence under subsection (1) is liable on conviction on indictment

(a) in the case of an individual to a fine of $100 000 or to imprisonment for a term of 10 years or to both; or

(b) in the case of a corporation to a fine of $250 000.

Malicious communications

19.(1) A person who intentionally or recklessly uses a computer system to publish, broadcast or transmit computer data that

(a) intimidates a person; or

(b) threatens to

(i) use violence towards a person or a member of his family; or

(ii) damage the property of a person or the property of his family,

is guilty of an offence and is liable

(A) **on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or**

(B) **on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.**

(2) A person who intentionally or recklessly uses a computer system

(a) to publish, broadcast or transmit data that includes private sexual photographs and videos without the consent of a person who appears in them, with intent to humiliate, harass or cause substantial emotional distress to that person; or

(b) to send repeatedly to another person data that is obscene, vulgar, profane, lewd or indecent with intent to humiliate or harass the other person to the detriment of that person's health, emotional well-being, self-esteem or reputation,

is guilty of an offence and is liable

(i) **on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or**

(ii) **on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.**

(3) A person who intentionally uses a computer system to disseminate any image or words **that are false** and causes or is likely to cause or subject a person to **humiliation or injury**, is guilty of an offence and is liable

(a) **on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or**

(b) **on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.**

(4) For the purposes of **this section**,

(a) "intimidate" means to cause

(i) in the mind of a reasonable person injury to himself, any member of his family or any of his dependants;

(ii) in the mind of a reasonable person an apprehension of violence or damage to any person or property; or

(iii) a person substantial emotional distress;

(b) "**injury**" includes injury or damage to a person in respect of his **reputation**, business, occupation, profession, employment or other source of income.

(5) The defences of truth, comment, triviality and privilege, whether absolute or qualified, provided for under the *Defamation Act*, Cap. 199 shall extend to a prosecution under subsection (3).

Cyber bullying

20.(1) **A person who intentionally uses a computer system to publish, broadcast or transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene or of a menacing character or causes any such data to be so sent for the purpose of causing danger, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress to that person is guilty of an offence and is liable**

(a) **on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or**

(b) **on conviction on indictment to a fine of $100 000 or to imprisonment for a term of 10 years or to both.**

(2) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act

(a) for a *bona fide* scientific or medical research or law enforcement; or

(b) in compliance of and in accordance with the terms of a court order issued in exercise of any power under this Act or any law.

Cyber terrorism

21.(1) A person who intentionally uses or causes to be accessed a computer system for the purpose of terrorism is guilty of an offence and is liable on conviction on indictment to imprisonment for a term of 25 years.

(2) For the purposes of this section, "terrorism" has the meaning assigned to it in section 3 of the *Anti-Terrorism Act*, Cap. 158.

Aiding or abetting

22. A person who aids or abets the commission of an offence under this Act is guilty of that offence and is liable to the penalty of that offence.

PART III

INVESTIGATION AND ENFORCEMENT

Search and seizure

23.(1) Where a Judge or magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for suspecting that an offence has been, is being or is about to be committed in any place and that there is evidence that such an offence has been, is being or is about to be committed in that place, the **Judge or** magistrate may issue a warrant authorising any police officer to enter and search that place, including any computer system, using such reasonable force as is necessary.

(2) A warrant issued under this section may authorise a police officer to

(a) seize or similarly secure any computer system, data, programme, information, document or thing if he reasonably believes that it is

evidence **or contains evidence** that an offence has been or is about to be committed;

(b) inspect and check the operation of any computer system referred to in paragraph *(a)*;

(c) use or cause to be used any computer system referred to in paragraph *(a)* to search any programme or data held in or available to such computer system;

(d) have access to any information, code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer system into readable and comprehensible format or text, for the purpose of investigating any offence;

(e) convert an encrypted programme or data held in another computer system at the place specified in the warrant, where there are reasonable grounds for believing that computer data connected with the commission of the offence may be stored in that other system;

(f) make and retain a copy of any programme or data held in the computer system referred to in paragraph *(a)* or *(e)* and any other programme or data held in the computer system;

(g) maintain the integrity of the relevant stored computer data; and

(h) render inaccessible or remove computer data from the computer system.

(3) Where a Judge or magistrate is satisfied on the basis of an application by the Commissioner of Police or other gazetted officer that specified computer data or other information is required for the purpose of a criminal investigation or criminal proceedings, the Judge or magistrate may order a person who has knowledge about the functioning of a computer system or measures applied to protect the computer data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the measures in subsections (1) and (2).

(4) A warrant issued under this section shall authorise an approved person or a person who has knowledge about the functioning of a computer system or measures applied to protect the computer data to assist a police officer in the execution of the warrant.

(5) A person who obstructs a police officer in the execution of his duty under this section or who fails to comply with a request under this section is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 2 years or to both.

(6) For the purposes of this section,

"encrypted programme or data" means a programme or data which has been transformed from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation and irrespective of the medium in which such programme or data occurs or can be found, for the purpose of protecting the content of such programme or data;

"plain text version" means a programme or original data before it has been transformed to an unreadable or incomprehensible format.

Assisting a police officer

24.(1) A person who

(a) is in possession or control of a computer data storage medium or computer system; or

(b) has knowledge about the functioning of a computer system or measures applied to protect the computer data therein,

that is the subject of a search or a seizure, shall assist a police officer in the execution of a warrant issued under section 23.

(2) The assistance referred to in subsection (1) may include the following:

(a) accessing and using a computer system or computer data storage medium to search any computer data available to or in the system;

(b) obtaining and copying computer data referred to in paragraph *(a)*;

(c) using equipment to make copies;

(d) obtaining access to decryption information necessary to decrypt computer data required for the purpose of investigating the commission of the offence;

(e) obtaining an intelligible output from a computer system in a plain text format that can be read by a person;

(f) maintaining the integrity of the computer data; and

(g) rendering inaccessible or removing computer data in the computer system.

(3) A person who fails without lawful excuse or justification to assist a police officer in accordance with subsection (1) is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 2 years or to both.

(4) A person who seeks to prevent or prevents another person from assisting a police officer in the execution of a warrant issued under section 23 is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of 2 years or to both.

(5) For the purposes of this section, "decryption information" means information or technology that enables a person to readily transform an encrypted programme or data from its unreadable and incomprehensible format to its plain text version.

Record of seized data to be provided to owner

25.(1) Where a computer system or computer data has been removed or rendered inaccessible to the owner or person who has control of the system

following a search or a seizure under section 23, the person who made the search shall, at the time of the search or as soon as practicable after the search,

(a) make a list of what has been seized or rendered inaccessible, with the date and time of the seizure; and

(b) give a copy of that list to

(i) the owner of the computer system or computer data;

(ii) the occupier of the premises; or

(iii) the person in control of the computer system or computer data.

(2) Subject to subsection (3), a police officer or an approved person shall, on request,

(a) permit a person who had the custody or control of the computer system, or someone acting on behalf of that person, to gain access to and copy computer data on the system; or

(b) give the person referred to in paragraph *(a)*, a copy of the computer data.

(3) A police officer or an approved person may refuse to give access to or provide copies of computer data referred to in subsection (2) if he has reasonable grounds for believing that giving the access or providing the copies

(a) would constitute a criminal offence; or

(b) would prejudice

(i) the investigation in connection with which the search and seizure was carried out;

(ii) another investigation connected to the one in respect of which the search and seizure was carried out; or

(iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations.

Production of data for criminal proceedings

26.(1) Where a Judge or magistrate is satisfied on the basis of an application by a police officer that specified computer data or other information is required for the purpose of a criminal investigation or criminal proceedings, the Judge or magistrate may order that

(a) a person shall submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; or

(b) a service provider offering services in Barbados produce subscriber information relating to such services that is in the service provider's possession or control.

(2) A person referred to in subsection (1) who discloses without authority any information in his possession or under his control is guilty of an offence and is liable on conviction on indictment,

(a) in the case of an individual, to a fine of $70 000 or to imprisonment for a term of 7 years or to both; or

(b) in the case of a corporation, to a fine of $250 000.

(3) For the purposes of subsection (1), "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic or content data, which can establish

(a) the type of communication service used;

(b) the technical provisions taken relating to the communication service;

(c) the period of service;

(d) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information on the basis of the service agreement or arrangement; and

(e) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Expedited preservation and partial disclosure of traffic data

27. Where a Judge or magistrate is satisfied on the basis of an *ex parte* application by the Commissioner of Police or other gazetted officer that specified data stored in a computer system is required for the purpose of a criminal investigation or criminal proceedings, the Judge or magistrate may make an order to ensure that expeditious

(a) preservation of traffic data is available regardless of whether one or more service providers was involved in the transmission of that communication; and

(b) disclosure of a sufficient amount of traffic data is given to enable the identification of

(i) the service providers; and

(ii) the path through which the communication was transmitted.

Preservation of data for criminal proceedings

28.(1) The Commissioner of Police or any other gazetted officer may make an *ex parte* application for a preservation order to a Judge or magistrate where

(a) computer data, including traffic data, stored in a computer system is required for the purposes of a criminal investigation; and

(b) there are grounds to believe that the computer data, including traffic data, stored in a computer system is particularly vulnerable to loss or modification.

(2) Where the Commissioner of Police or any other gazetted officer satisfies a Judge or magistrate on the basis of an *ex parte* application made under

subsection (1), the Judge or magistrate may make an order requiring the person in control of the computer system to

(a) ensure that the computer data specified in the order is preserved for a period of up to 90 days;

(b) maintain the integrity of the computer data for a period of up to 90 days; and

(c) keep confidential any information or action relating to the preservation order.

(3) Where the Commissioner of Police or other gazetted officer makes an *ex parte* application for an extension of a preservation order, a Judge or magistrate may extend the preservation order beyond the 90 day period for a further period of up to 90 days.

Order for payment of compensation

29.(1) The Court may make an order for the payment of compensation where a person is convicted of any offence and he causes damage to another person's computer system, programme or data.

(2) A claim by a person for damages sustained by reason of the offence is deemed to have been satisfied to the extent of any amount which has been paid to that person under an order for compensation.

(3) An order made under subsection (1) shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.

(4) An order for compensation under this section is recoverable as a civil debt.

(5) For the purposes of this section, a programme or data held in a computer system is deemed to be the property of the owner of the computer system.

Regulations

30. The Minister may make regulations generally for the purpose of giving effect to this Act.

Consequential amendments

31. The enactments set out in the first column of the *Schedule* are amended in the manner set out opposite thereto in the second column.

Repeal

32. The *Computer Misuse Act*, Cap. 124B is repealed.

Commencement

33. This Act shall come into operation on a date to be fixed by Proclamation.

SCHEDULE

(Section 31)

CONSEQUENTIAL AMENDMENTS

Column 1	Column 2
Enactment	*Amendment*
Copyright Act, Cap. 300	In section 31
	(a) delete subsection (5) and substitute the following: "(5) Copyright in a work is infringed by a person who, without the licence of the copyright owner, transmits the work by means of a computer system or telecommunications system (otherwise than by broadcasting or inclusion in a cable programme service) knowing or having reason to believe that infringing copies of the work will be made by means of the reception of the transmission in Barbados or elsewhere.".
	(b) insert immediately after subsection (5) the following new subsection: "(5A) For the purposes of subsection (5) "computer system" means a device or a group of interconnected or related devices, one or more of which, pursuant to a programme, facilititates communication, performs automatic processing of data or any other function.".

Schedule - (Concl'd)

CONSEQUENTIAL AMENDMENTS - *(Concl'd)*

Column 1 *Enactment*	Column 2 *Amendment*
Defamation Act, Cap. 199	Section 34 is deleted.
Extradition Act, Cap. 189	*(a)* In section 4, insert immediately after subsection (2) the following new subsection: "(3) An order made under subsection (2) shall be subject to affirmative resolution.". *(b)* In the *Schedule* insert immediately after paragraph 40 the following new paragraph: "41. Any offence under the *Cybercrime Act*, 2024 (2024-).".

HANSARD TRANSCRIPTS

PRELIMINARY & 1st MEETING
JOINT SELECT COMMITTEE (STANDING)
ON
GOVERNANCE AND POLICY MATTERS
ON THE
CYBERCRIME BILL, 2024
AND THE
MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024

Monday April 8th, 2024

PRESENT WERE:

Mr. E. G. HINKSON, S.C., M.P., LL.B. (Hons.), L.E.C., LL.M., (CHAIRMAN)
Dr. R. O. SPRINGER, J.P., Ph. D. (DEPUTY CHAIRMAN)
Mr. P. R. PHILLIPS, M.P., J.P.
Senator G. P. B. NICHOLLS, B.Sc. (Hons.), LL.B. (Hons.), LL.M., MCIArb.
Senator the Hon. L. E. NURSE, F.C.A., F.C.C.A.

ALSO IN ATTENDANCE WERE:
Mr. Pedro Eastmond (Clerk of Parliament)
Ms. Beverley S. GIBBONS (Deputy Clerk of Parliament)
Ms. Suzanne Hamblin (Assistant to the Clerk of Joint Select Committees)

ABSENT:

Mr. R. A. THORNE, K.C., M.P., LL.B., L. E. C., Dip. Theology (Leader of the Opposition)
Senator R. O. WALTERS, MBA.

Call to Order

Mr. CLERK: At this time, I would entertain a motion for the appointment of the Chairman of the Committee.

Senator G. P. B. NICHOLLS: I would like to propose Mr. Edmund Hinkson S.C., as Chair.

Mr. CLERK: A seconder please.

Dr. R. O. SPRINGER: I second that.

The question to appoint a Chairman was called by Senator G. P. B. NICHOLLS and seconded by Dr. R. O. SPRINGER was resolved in the affirmative without division.

Mr. CLERK: Mr. Edmund Hinkson has been appointed as Chairman for this Committee. Mr. Hinkson, you have been appointed and I invite you therefore to sit next to me and Chair the meeting.

Mr. CHAIRMAN: I thank members for your confidence to elect me as Chairman.

Asides.

Mr. CHAIRMAN: The appointment of Deputy Chairman is now up for consideration. I take proposals from the floor.

Senator G. P. B. NICHOLLS: I would like to propose Dr. Romel Springer.

Senator the Hon. L. E. NURSE: Seconded.

Mr. CHAIRMAN: Okay so the proposal is for Dr. Romel Springer, to be Deputy Chairman. Do you accept? Okay. So essentially, the background to the Committee and the probe into these two (2) Bills arises from the Cybercrime Bill passing the Lower House but at the Upper House level, it was decided to send it to this Committee – Governance and Policy Committee -- for consideration and for the public to be allowed to make oral and written presentations in the forms that would be for consideration under the next Item of Agenda. The Mutual Assistance in

Cybercrime in Criminal Matters Amendment Bill, what was the position with that Mr. Eastmond?

Mr. CLERK: Mr. Chairman, as you realise in the Lower House both Bills were debated as a cognate debate so once one was sent, both were sent to this Committee.

Mr. CHAIRMAN: For consideration, now is Item No. 2 on the Agenda, the Terms of Reference of the Committee and examination of these Bills and we would have sent, I believe Parliament would have sent, a draft Terms of Reference for consideration. I made a slight change last night, so I just was wondering if that was sent out as well this morning?

Asides.

Mr. CHAIRMAN: You have the latest because we did not pick up that Cybercrime was spelt wrong, so you have the latest now, so I just wanted to be sure.

Mr. CLERK: But no change in substance?

Mr. CHAIRMAN: There was a slight change in substance. Remove 'police'. You have the correct one, so this one went to Committee Members?

Asides.

Mr. CHAIRMAN: We could examine these Terms of Reference. Does anyone wish to propose any addition or missing amendment to the eight items there for us to inquire into? I would essentially have drafted these from what I saw as the concerns and criticisms of certain sections of the Bill on Social Media; to give those who object and wish the opportunity to come and state why they have these concerns or criticisms.

Dr. R. O. SPRINGER: Item five. I am wondering if we should look at the Bill also from a gender perspective. I find a lot of the victims of cybercrime, certainly in this country and across the world, are females. I think that should be a consideration separate from … it should actually be added to the list here, where we look at the impact of females or at least on gender and we could focus on females, as it relates to this particular Bill.

Mr. CHAIRMAN: So what would you propose? How would you word that as a separate…?

Dr. R. O. SPRINGER: It has whistle-blowers as a special area where we should query if the Bill provides adequate protection or cover. I think that we can also work it into that particular item there for whistle-blowers for women.

Mr. CHAIRMAN: If anything I think it would have to be a separate one as you were proposing. We need to examine whether the Cybercrime Bill as drafted, provides adequate protection. You would want to say specifically for females or on the basis of gender?

Dr. R. O. SPRINGER: Sir, I would say on the basis of gender just to be publicly correct but I am thinking more of women and girls but to be correct and to be fair and balanced, you would have to say gender.

Mr. CHAIRMAN: Okay. What do other Committee members think of that?

Senator G. P. B. NICHOLLS: Mr. Chairman, I understand what Dr. Springer is saying but I am not sure why it has to be a specific Term of Reference. I am not sure I am getting exactly what he is saying. I am not sure. I understand that cybercrime affects people all across the spectrum; people of all genders; all races; all classes and so and to identify one characteristic of people, as to be the specific focus of the Committee to my mind; I mean there is anecdotal evidence that suggests that the levels of suicide were as a result of cybercrime last year and that from the anecdotal evidence available was disproportionately moreso in favour of men and particular type of men and that is just from the anecdotal evidence that we had going on. Nobody has done any complete study. While I do not want to disagree with him, I think what he said is a very valid concern; that we need to be able to examine the scope of the legislation as it affects people who are affected generally by it and women tend to be in terms of revenge porn and all the other different things.

We must be careful that our Terms of Reference do not necessarily and unwittingly, exclude other valid places of enquiry that we should ourselves examine because the legislation is going to have to function as a criminal statute that is going to penalise behaviour that is abhorrent to the society as a whole, as it relates to whole sets of other people.

The Terms of Reference have to be drafted, in my view, in as broad a way as is necessary to reflect the parliamentary intent because when there is any ambiguity or doubt as it relates to how the legislation ought to be interpreted, these Terms of Reference and the Report of the Committee might unwittingly find their way into a determination that the scope of the legislation was not intended to cover other groups and be special focus at the time of the Parliament.

We are not talking about a review of the legislation next year or the next two or three years but suppose this goes on the books for 20 years or 30 years from now when we are all long gone, then, it will be that when we look back at the Terms of Reference, it was with specific focus on women and was not an issue then or it might be skew…

Mr. Chairman, I am just saying that while I accept what Dr. Springer is saying and I take his suggestion that we speak and say "gender" but the truth is that "gender" in law has a different connotation and does not necessarily include "male" and "female" as well. We have to be very careful that "sex" and "gender"; while we might mean "sex"; people might talk about "gender" and then does "gender" include "gender identity"? Does "gender identity" include "gender fluidity"? Then we could just go down the line.

I am not saying that I am trying to trivialise it but there are important constituent groups out there to whom these nomenclatures mean a lot and we have to be very careful that by what we are doing, we are not excluding that which may be the very subject of the cybercrime that we are trying to prevent; so I am in agreement with Dr. Springer that we perhaps we need to ensure that the Terms of Reference be as broad to cover and not exclude any of the categories because there are a lot of people who are affected generally by cybercrime. There is a lot of under-reporting of how minorities in various categories are treated by the society generally and this is something that we want to make sure that people who are the subject of cybercrime, are given adequate protection. Thank you!

Dr. R. O. SPRINGER: You are the lawyer. Would vulnerable groups which would include those various groupings in society; females, cover the issue of gender? Would a term like that be satisfactory because it speaks to those persons who are disadvantaged in society? What I am trying to do is to ensure that in the same way that we pay special attention to whistle-blowers, I mean, that is going to speak to the other Bill, but that we have a category that looks within these Terms of Reference at those groups within the society that ultimately would suffer more as a result of a violation of this legislation.

Mr. CHAIRMAN: As I said, I put in whistle-blowers there because that seemed to be a concerned of one of the critics on Social Media, that there was not adequate or enough protection for whistle-blowers but I have not seen that anyone has criticised the Bill on the basis that there was not adequate or enough protection for females. I take Senator Nicholls' point because if you put in females alone, yes, the issue comes up, the homosexuals; then the transgender and that will be the dilemma there. What is your opinion Senator Nurse?

Senator the Hon. L. E. NURSE: Actually, I am in general agreement with Senator Nicholls' further comments. The only thing I would ask is if, in drafting these, if we had gone back and had a look at what was discussed and the Resolution that came into the Honourable The Senate, to say specifically, if there were any instructions which they may have given for the Committee to specifically consider.

Mr. CHAIRMAN: Was there a Resolution before the Senate on it? Okay.

Mr. CLERK: Mr. Chairman, before we get to the Resolution, I was thinking that we could widen the third Term of Reference because it speaks to potential abuses but it only refers to abuses of non-enforcement power rather than abuses generally so I was thinking that maybe that term "Term of Reference" could cover abuses in addition to the law enforcement ones.

Mr. CHAIRMAN: "*From potential abuses including the expansive of law enforcement powers*?" Is that how you would want to word that?

Asides.

Mr. CHAIRMAN: I am asking Mr. Clerk, if then:

"… liberties and privacy rights from potential abuses, including expansive law enforcement powers …".

Is that your thinking?

Mr. CLERK: Yes, I was thinking that we could add that. I do not know what the members think about that.

Dr. R. O. SPRINGER: I have no difficulty with it.

Mr. CHAIRMAN: Senator Nurse, are you good with that?

Senator the Hon. L. E. NURSE: Yes.

(Mr. P. R. PHILLIPS joined the meeting.)

Mr. CHAIRMAN: Welcome Mr. Phillips. An amendment to the third term "… *and privacy rights from potential abuses, including from expansive law enforcement powers, in order to prevent miscarriages of justices …"* but still to make a decision on Dr. Springer's proposal. I think we accept Senator Nicholls' point that we should not specify gender when there are other vulnerable groups, gender identity, that are vulnerable too. Is there a feeling that we need to put in something to protect the "vulnerable groups", period? Technically, every group is a vulnerable group so I am wondering if …

Senator G. P. B. NICHOLLS: Perhaps, if we could say something along the lines that we should examine whether the provisions of the Bill give adequate protection to any special classes or groups of persons who might be victims of cybercrime and then you can identify the specific elements of it and leave it there. If you want, you could include a list of the groups but do not make that listing exhaustive of the scope of that inquiry. I do not know if the recorders captured that, but if you ask me to repeat it, I am not going to be able to repeat it.

Mr. CHAIRMAN: You could repeat it by proposing the …

Senator G. P. B. NICHOLLS: I just proposed that as the additional category.

Mr. CHAIRMAN: Right, to word it: To examine whether the Cybercrime Bill as drafted…

Senator G. P. B. NICHOLLS: … provides adequate protection in the law for any persons who might be targets of or unduly affected by cybercrime, and you can name these specific types of cybercrime that we are talking about. I cannot remember all. There is cyber-bullying.

Mr. CHAIRMAN: You may not want to name them. Just leave it general.

Senator G. P. B. NICHOLLS: We can add women but not to make it exclusive, if you want.

Mr. CHAIRMAN: That is why I was saying maybe do not add any at all. Maybe you can say: *"To examine whether the Cybercrime Bill as drafted provides adequate protection for…."*

Senator G. P. B. NICHOLLS: …"p*ersons who are targeted or exposed to cybercrime or acts of hatred online, as a result of any characteristics that divide them into a particular class"*. If you try to avoid the elephant in the room, you will avoid it and you will not end up getting what you want.

Mr. CHAIRMAN: Yes. Specific categories of persons.

Senator G. P. B. NICHOLLS: I think the first formulation I had may have captured it a little better.

Mr. CHAIRMAN: Right. Specific categories of persons who may be most vulnerable to cybercrime?

Senator G. P. B. NICHOLLS: Yes.

Mr. CHAIRMAN: People understand what that is without having to define….

Senator G. P. B. NICHOLLS: …who the people are.

Mr. CHAIRMAN: Right.

Dr. R. O. SPRINGER: In giving it further thought, this would also group gender, and include women, females and children but a lot of young persons who are victims of cyber-bullying are teenagers, schoolchildren; there is also that group who may not necessarily fit into a particular category of people but who certainly have been among the victims of cybercrime. How we word it should be such that we can capture all of the various groups of persons within the society who historically and traditionally have been the victims of bullying in its traditional sense and now cyber-bullying as it has now been defined.

Mr. CHAIRMAN: Mr. Phillips, we welcome you. We are looking at the Terms of Reference that will define our work. Earlier, I was elected as Chairman and Dr. Springer as

Deputy Chairman. We are looking to see if the draft Terms of Reference before us, need to be amended; omitted or added. It seems to be the feeling that we should add another Clause.

Senator G. P. B. NICHOLLS: Mr. Chairman, before we conclude on that Clause, when the Deputy Chairman was just speaking, I remembered that there is some concern that the legislation may not provide the range in terms of punishments. That is, not all cyber activity is a cybercrime and there is a level of subjectivity in the Bill, in my view, that had the Bill been passed in its present form, I fear it would have been struck down by the courts for being too vague.

A person needs to know that a particular act that they are engaging in is criminal. When a person does an act and does not know that it is criminal and by any objective standard, it can be questionable whether it is criminal. In other words, if two people looking at the same act can have genuine views that one might think it is a crime and the other might think it is not, or whether it is up to a policeman or officer of the State to determine whether that action constitutes a crime; or whether somebody who may be apprehended that there is some danger or fear to them, that might not be readily understandable by other people; that level of vagueness would lead to the law to being struck down.

I am not saying that because I am anti- the Bill because I am not, but I am cognisant of the fact that, for example, the cross-dressing law in Guyana was struck down two years ago by our highest court; where for a man to put on women's clothing and stand on the street, itself is not a crime but it was made into a crime. There was a view that men should not be standing on street corners dressed in women's clothes and police used to move people doing that for many years but it was not a crime but it made its way into a law or there was an old law that was struck down by the Savings law; something like that.

Similarly, last year the offence of wandering; that has been a crime since the 1800s, was struck down last year by our courts here in Barbados. Wandering is only something that a child can do. An adult cannot wander. If any of us go outside and did what a child was doing, it would be normal but for a child it was a crime and the courts struck it down within the same principle. There is another example, there is something called **ethical hacking**; where people actually go into your own business and programmes and computer without permission and then develop the mechanism to tell you, "*Brother Nurse, you are selling a product here but these are the flaws in your system*," and sell you the programme to keep people from breaking into it; because we have hacked into your thing and this is how we can defend it.

Our legislation seems to criminalise that action, and without ethical hackers, a lot of the hackers could never be prevented from hacking in the first place. When you do some research into this, I wonder whether or not there is a level of subjectivity in terms of what is a criminal offence; the level of uncertainty and vagueness and also the complete, absolute no-go areas, where we are not allowing for the hackers to develop alongside the technology. You are pre-supposing that the owner of every technological device has the capacity to determine its strength and weakness and that is not so. The only way I can know that your thing is compromised is if somebody breaks into it or unless you engage somebody to test it for you.

Those are my concerns, Sir, and I think this is something we should be concerned about because the truth is that, no matter what international convention we follow, this thing is moving every day because we are dealing with the world of technology. The truth is that we cannot have laws that are preset to deal with criminal activity in the last century dealing with laws that are for this century; the same modalities without the necessary flexibility in there.

If a policeman determines that your looking into Social Media and somebody sends you a feed or something that you open and they happen to ask you to open your phone and then you realise, *"This is something I was watching on Social Media that everybody is watching*" but you get locked up for watching what 10 000 people have watched. Is that the kind of behaviour we are intending to criminalise? Is that what is intended to be captured by the legislation?

I am not trying to say it is, but watching it can be argued to be a crime. Without intending to distribute or any such thing and it can be proven that you have opened this thing – you could have opened it, seen it and then turned it off at the same time – somebody can retrieve your data and see

that you have opened or accessed a site. You looked at it for two seconds but does the Act say that when you have looked at it for two seconds it is not a crime, as opposed to watching it for the entire thing? Or watching it and forming the view that this is distasteful and should not be on the thing? The policeman can just decide and say, "*But oh, you watched it though. So you are a criminal."* Is that the intention of the legislation?

I am just wondering if we should not only examine the things here, Mr. Chairman. In coming home now, should we not inquire whether the legislation is overly broad, subjective, vague in its criminalisation of behaviours which are not necessarily of a cybercrime nature?

In my own research, there are two types of cybercrime. There are the crimes that are normal crimes that are assisted. I think they are called computer-assisted crimes. It would be a crime normally but you are just using a computer to perpetrate the crime. There are crimes then that could only be done on a computer. We need to make sure that in creating this omnibus Bill that we do not take the mechanisms for normal crimes, you do not need a computer to commit these crimes but they can be committed on a computer. You are not taking that methodology and then, transporting it to a situation where this crime could only be committed on a computer and creating a bridge between the two and then you are sweeping everything under...this is a big discussion going on all over the world right now. The present debate is not on the Convention that we are modelling this legislation on. Presently, the United Nations (UN) is in debate and discussion on an international Convention which goes even further than the European one. There is a big debate. We are putting in place legislation to deal with something that is only existing in Europe while not listening to the debates about the challenges with implementing the international Convention that the UN is debating at present. I want to know if you want to be able to look at these times because this is not something we can fiddle around with. This is going to be an important piece of legislation that is going to govern a lot of the 21st Century life as we know it.

I think we have to be very deliberate in our deliberations about its scope, its effectiveness and its reach, without necessarily letting down the vulnerable in the society but at the same time, not intruding on the rights of persons who are not necessarily the targets of the legislative action which we are engaging in. Thank you, Mr. Chairman.

Mr. CHAIRMAN: Thank you, Senator. We are going to consider certainly what you just said but let us settle first on the earlier one to see if we could get that

wording and then we are going to address what you just said which obviously has merit too.

Mr. CLERK: Mr. Chairman, just following up on what Senator Nurse had asked in relation to the Resolution in the Senate. All the Resolution in the Senate really did was to encourage that the Bill be sent to Joint Select Committee so that a fuller discourse of the Bill could be undertaken. So, it did not….

Mr. CHAIRMAN: Okay. Let us see if we could agree on this wording to put a new No. 5, I would propose, *"to examine whether the Cybercrime Bill, as drafted, provides adequate protection to all of the specific categories of persons who may potentially be vulnerable to cybercrime."*

Does that adequately catch what Dr. Springer was proposing and what the Committee seemed to agree should be fitted in some way, without specifically defining or identifying any of these specific categories of persons? How does that sound?

"*To examine whether the Cybercrime Bill, as drafted, provides adequate protection for all….*

Did I say all? *To examine whether the Cybercrime Bill, as drafted, provides adequate protection for all of the specific categories of persons who may….*

Do we want to use the word *"potentially*"? Or omit *potentially*? *To examine whether the Cybercrime Bill, as drafted, provides adequate protection for all of the specific categories of persons who may potentially be vulnerable to cybercrime?* Do you want to use the word "potentially" or omit that? Including "potentially"?

Dr. R. O. SPRINGER: If you remove "potentially" in this particular case, it does not change the objective of the particular sentence in any way.

Mr. CHAIRMAN: Alright. So we put that in as No. 5 and then Senator Nicholls' concern. Maybe, we could move the existing No. 4 further down after the whistle-blowers. Pardon me. No. 5 then becomes No. 6 because we have a new No. 5. To move No. 4 down then to…. The No. 1 that I just said could be No. 4. No. 5 would remain where it is and No. 4 comes down. Senator Nicholls, let us see how we are going to word yours then. *"To examine whether any of the provisions in the Cybercrime Bill, as drafted, are vague and/or uncertain, in accordance with the standards of criminal law?"*

I know we can get better wording of that but is that the gist, Senator Nicholls, of what….

SENATOR G. P. B. NICHOLLS: Not necessarily of criminal law because you want to … avoid vague or arbitrary laws altogether and not necessarily only in the criminal section because there is some kind of civil liability being created around the legislation too or could be created by the legislation too; the basis any civil action where a person might use a conviction as the basis to assert a civil right later on. I would not put the word "criminal" in. We want to review the legislation to determine whether or not the provisions of the Bill are arbitrary, vague or run afoul of the rules that prevent laws from being vague, uncertain or arbitrary in terms of the level of liability that they impose on people; or are overly broad. That is another concern -- that we just have this broad brush approach, that everything that could be a computer crime is now covered by this Bill. For example, I think some of my colleagues who sit on the Independence Committee had this concern: If the police want to come into your house they need to have a search warrant; refusing to allow them entry is not a crime but refusing to allow the police to access your cell phone is a crime, without a warrant. That in itself is made a crime in this Bill. That could not be the legislative intent.

Some policemen that just do not like you would say, "*I want to see your phone!*" And you say, "*No, you cannot use my phone*!" That is a crime now, even though there is no underlying criminal action. That is why we are trying to make sure that we are not using this broad brush approach to capture the people who are grooming children and that kind of stuff who might look innocent; like the priests and the teachers and who might be in positions of trust. The Scout leader and the Girl Guide leader, who may be a good girl in the Church but her cellphone is full of porn; child pornography.

Yes, we want to capture those persons, but should an ordinary person who refuses to allow the police to look at their phone, does that act and that act alone satisfy us that it needs to be a criminal sanction? We would have to line up people outside the court everyday with the police, if we really think about this. Sorry, but I came with my shopping list. In other societies, it is the duty of the government to issue executive guidelines and I think we need to put some scope to that in this legislation.

What do I mean by *Executive Guidelines*? What is the policy? The police would not arrest people for not showing them their cellphones. The police will not do this; the police would not do that and those are the guidelines that a society would accept and I think some of the groups out there would want to know that it is not left to the discretion of the Commissioner of Police to get up today and say "*Fellas don't do this or that'*, but that there is published, detailed guidelines that are reviewed consistently over time, so citizens would know well look if we go down this road it may or may not be illegal and stuff like that but at least we know that the fellow with a spliff smoking on the street knows that the police will not arrest him anymore because there is kind of an unwritten policy that he is not going to trouble a guy with a single spliff, right? If he is down at the beach at 3 o'clock in the morning with a boat coming in and you are found with a big garbage bag, chances are the police would likely stop you so we need to be able to establish the guidelines as to how people can conduct themselves.

That way the certainty in the legislation is guaranteed. That is where I am coming at Chair, in terms of the broad, varied, subjective, arbitrary, all these things that we want to avoid because the legislation is too important to just dump it but I fear if you do not tighten up some of these things, the court might not be able and the Clerk would tell you and Mr. Chairman, you would know. If the court cannot sever the offending provisions, you know what happens? The entire Bill is struck out.

Asides

Senator G. P. B. NICHOLLS: Pardon? Reduce it to a Term of Reference?

Mr. CHAIRMAN: Yes, because No. 3 in your opinion, does not adequately cover what you just said.

Senator G. P. B. NICHOLLS: No, and we want the public to see that this is what we are concerned with ourselves. I am not saying that I would be able to convince all of the Members of the Committee to my views but I think that when we discuss it; I could take you through the examples as to why certain things in the Act might not pass, and if we need to get at a particular evil or wrong, we need to cover it in correct language.

Mr. CHAIRMAN: "*To examine whether the Cybercrime Bill that is drafted provides*," sorry; *to examine whether any of the provisions of the Cybercrime Bill as drafted, are vague, broad, arbitrary and/or uncertain…*

Senator G. P. B. NICHOLLS: Mr. Chairman, I would go with 'overly broad'.

Mr. CHAIRMAN: *…overly broad and/or uncertain, in its imposition of liability*, and you do not want to say criminal liability, so would that do?

Senator G. P. B. NICHOLLS: Yes, Mr. Chairman. Very much so.

Mr. CHAIRMAN: *To examine whether any of the provisions of the Cybercrime Bill as drafted, are vague or too vague*?

Senator G. P. B. NICHOLLS: Vague.

Mr. CHAIRMAN: *Vague, overly broad, arbitrary and/or uncertain?*

Senator G. P. B. NICHOLLS: *Subjective or uncertain*?

Mr. CHAIRMAN: Subjective as well? Alright. *Subjective and/or uncertain, in its imposition of liability.* We want to put that then as a new No. 4 after No. 3. Sorry?

Asides

Mr. CHAIRMAN: No. 5? Okay. So to put that as No. 5. Whistle-blowers as No. 6 and then the penalties which is at No. 4, as No. 7, alright. Everyone comfortable with that? Any other proposed amendments or additions?

Senator G. P. B. NICHOLLS: Mr. Chairman, I just want to add ethical hackers to No. 6. You talk about impeding technology unless you can say that the ethical hackers could be in there but I do not know if that is broad enough or if you want to be able … ethical hackers if you do any research on this is a big thing in the cyber world.

Mr. CHAIRMAN: Reword No. 6?

Senator G. P. B. NICHOLLS: "*…could impede innovation in the technological sector and discourage investment and research, including research by ethical hackers*."

Dr. R. O. SPRINGER: Just to chime in here quickly. I know the term ethical hackers is a term now but the concept of an "ethical hacker", I have a difficulty with, in terms of a person who could be considered ethical today or ethical with you, might be ethical with her or with me but be unethical tomorrow. I guess that one, even though I understand the concept and how it could work; that person still to me, is on the brink of breaking the law, especially if they do not get what they want. I do not want to create any comfort for a person who believes they could hack into your system and then either propose to you or threaten you, because they can do that; they have the ability to do that; that they can either improve your system; security or wipe out your system. We do not want to create any comfort, even a small opening.

Senator G. P. B. NICHOLLS: I understand you, Dr. Springer but the truth is, that somebody could be listening to what we are doing here with our own devices and not connected to Parliament's system. Trust me and probably there may be someone in the world watching us sitting down here, right, and they are obviously breaking the law; but the next technology that you start to utilise, chances are, that it has been developed by virtue of that person being able to understand what walls they need to go through and there is a lot of documentation. You are not saying that we are permitting it, because for example, I am not being farfetched but the person who develops technology for **Google** or whatever; could be extradited to Barbados under this legislation, if possible and brought before the Barbados courts, while they have been responsible for the mass of technology out there that has been helpful and not disruptive.

It is not to say that a person in Barbados can say, use the "ethical hacking" defence but what

you do not want is a person who is legitimately engaged in that practice, to be caught by the legislation, on the basis that you went into somebody's data. You are not encouraging people to go into your data but do you want to criminalise those persons who by going into your data and are developing the technology that allows us to have some modicum of privacy? An ethical hacker is not a 'cop out'. It is not an excuse; it is not a, *"I will use this as a convenient defence"*. Ethical hacking is a legitimate practice.

Mr. E. G. HINKSON: What about just adding *to discourage investment and research?*

Senator G. P. B. NICHOLLS: Yes.

Mr. E. G. HINKSON: Put in the words *"and research*" in there after "*investment*".

Senator G. P. B. NICHOLLS: Mr. Chairman, again, I am not saying this because … this is not a shopping list … As I said, these are concerns that have been raised and are in raging debates right now in the international sphere and we owe a duty to the people that the legislation that we bring into play is cognisant of the current ongoing discussions at all levels. I am not just here to review or to see whether the drafters got it right.

Mr. E. G. HINKSON: Remember that there is the all-embracing No. 8 and obviously that is going to come down; but are there any other recommended changes, as we go through the whole process and inquiry.

Dr. R. O. SPRINGER: There is something, Mr. Chairman, that Senator Nicholls said earlier that is a logic; a thought process that I want to respond to you as it relates to ethical hacking. It is one of those crimes that is only legal online but would be illegal in the real world. Just like there are certain things that would be legal for adults but would be illegal for children or would be illegal online but legal in the world.

If I break into your house and I determine that I can come up with a better way of securing your house; maybe better locks; maybe a better security system; cameras and all such like, if I do that, I am committing a crime, whether I go in there just to prove that I can get in and then come back to you and advise you on how to best secure your property, I am still committing a crime; I am still trespassing; I am still breaking and entering and that is in the real world. Because you do it in cyber space does not make it any less of a crime but that is just my take on something that as said by you earlier, just to reverse it. I understand it; it is research; it is innovation but I do not want to use that term at all in the Terms of Reference. We know what we are referring to when we speak of research but we would not use that particular term.

Mr. CHAIRMAN: So you do not agree with adding *research*?

Dr. R. O. SPRINGER: No, no, no, no. Just the term. No. I am agreeing.

Mr. CHAIRMAN: Oh, the *ethical hacking*? Not to use that.

Dr. R. O. SPRINGER: Yes. I am agreeing "*adding research*" just not the …

Mr. CHAIRMAN: Research added and that No. 6 now becomes No. 8, right? Yes. That would now become No. 8. Alright.

In terms of the Mutual Assistance in Criminal Matters (Amendment) Bill which was the penultimate item. Are you comfortable with that?

That is the purpose of that Bill in the Short Title. Like I said, the last one here in the draft is all- embracing. Anything else that we agree on at the end to make any further changes. Are we in agreement on the draft as amended? I know, Mr. Eastmond, that when you send out your document, you would send a clean one, right?

Mr. CLERK: Yes.

Mr. CHAIRMAN: Okay, so No. 3: **Scope of Works**. How are we going to go about our work and our examination and investigation? Of course, this is the second hearing under the new system of Select Committees right? At least define Committees now because we are at the Environment and Social Sector Committee examining the Child Justice and Child Protection Bills. It seems the first thing would be, just to follow their precedent, would be to write specific organisations and interest groups, individuals who we have seen and have expressed concern or criticism of some provisions or aspect of the Bill. So do we agree to do that as well, inviting them to come before us to make either oral presentations or written? I would propose the Democratic Labour Party (DLP) because they seem to have

something to say on it and their spokesman, if I remember and from what I saw on Social Media, Ms. Felicia Dujon, who I believe is their third Vice President, …

Senator G. P. B. NICHOLLS: Invite the Party and not any individuals.

Mr. CHAIRMAN: Yes, the Party itself. I was just giving that background, that she seemed to speak so we will invite the Democratic Labour Party.

Mr. CLERK: Mr. Chairman, before you go on. The first organisation that we need to have here is the Chief Parliamentary Counsel (CPC), our representative, to certainly partner with us throughout the investigation by the Committee because if any changes are suggested, they would be the ones who have to make the changes.

Mr. CHAIRMAN: So, the Chief Parliamentary Counsel or a representative would attend every hearing?

Mr. CLERK: Yes, as technical support and advising the Committee on the Bills and the instructions because many times when Committee Members express concern about a provision as drafted, they are the ones who would provide the reason why it was drafted in the way it was drafted.

Mr. CHAIRMAN: Fair enough. When we had a session on the draft Rights of Persons with Disabilities Bill, they were present as well. I would also propose, Sir David Simmons, who had a role in the crafting of the Bill. Is that correct?

Senator G. P. B. NICHOLLS: As the Law Reform Commissioner?

Mr. CHAIRMAN: As Chairman of the Law Reform Commission. Do we invite him specifically as the Chairman? How would you propose that it is done?

Mr. CLERK: I do not think that we used the Law Reform Commission at all, but if the Committee wants to have them.

Mr. CHAIRMAN: They had a role.

Mr. CLERK: No. I meant that you were making a reference to the previous Committee.

Mr. CHAIRMAN: Oh! No. They did not come, but in this case, I know they had a role.

Mr. CLERK: Then you could invite him as the Chairman of the Law Reform Commission.

Mr. CHAIRMAN: Yes, so the Chairman of the Law Reform Commission; the Democratic Labour Party (D.L.P.); Mr. Neil Harper. I do not know him but he obviously critically analysed it. I am assuming you all (Parliamentary staff) can get his details.

Senator G. P. B. NICHOLLS: Mr. Chairman, why not invite the major political parties. There is the Barbados Labour Party (BLP), there may be Bishop Atherley's party or whatever remnants there is, …

Mr. CHAIRMAN: I was thinking of Bishop Atherley's Party too.

Senator G. P. B. NICHOLLS: Yes, but invite all the known political parties and actors because the intention here, as I understand it, is to get a broad consensus from the public about any concerns in respect to the Bill.

Mr. CHAIRMAN: Right. So the Barbados Labour Party as well; and these letters would go to the General Secretary of each of the political parties. In Bishop Atherley's case, you would have to write him directly. I do not know who the General Secretary is. The three political parties.

Mr. CLERK: This Bill was passed in the House of Assembly by the Barbados Labour Party.

Senator G.P.B. NICHOLLS: No, it was passed by the Government.

Mr. CLERK: Do you want to invite them still?

Mr. CHAIRMAN: The body can decline to come.

Senator G. P. B. NICHOLLS: The two are not the same. I understand what you are saying in relation to the Barbados Labour Party and the Government but the two are not the same. I also believe you should invite the media because media practitioners have expressed some views as to whether or not this is an encroachment on their ability to practise their profession.

Mr. CHAIRMAN: The media is there within the three.

Senator G. P. B. NICHOLLS: Okay.

Dr. R. O. SPRINGER: We should invite what we call some of those people; influencers?

Senator G. P. B. NICHOLLS: Social media bloggers?

Dr. R. O. SPRINGER: Those persons, yes.

Mr. CLERK: Do you have any names of these bloggers?

Senator G. P. B. NICHOLLS: When we said you would invite the DLP, I thought that would have covered all of them.

Asides.

Mr. CHAIRMAN: There is a Peter Thompson as well.

Dr. R. O. SPRINGER: Stephanie Chase.

Mr. CHAIRMAN: Again, I do not know Peter Thompson but I presume that you would find it on Social Media. Peter Thompson, he also was pretty critical. There was also Mr. Cammie Holder, who is known and we can easily find him. What about Mrs. Marcia Weekes? Would she come into this as well?

Senator G. P. B. NICHOLLS: Mr. Chairman, we should put a notice out to invite people but is it that we are targeting people to come to us? Specific individuals?

Mr. CHAIRMAN: Yes, I think that was what you did with the Social Justice Committee. Who did you all invite?

Asides.

Mr. CHAIRMAN: Yes, so let us invite all of these people who I am calling. I mean, it is their choice to come or not. It is their choice if they want to write in.

Asides.

Mr. CHAIRMAN: I would want to say the media houses, invite each of them, so that would be the **Nation**; **Starcom**; **Caribbean Broadcasting Corporation**; **Barbados Today**. Like I said, what about Mrs. Marcia Weekes? She has a show, I believe, so invite her too? Okay, the point the Clerk was making and what I am saying is, that with the Social Justice Committee they had political parties, Democratic Labour Party and People's Party for Democracy (PdP); no Barbados Labour Party but I would still want to say write the BLP too. They may say 'no' but we stand by the Bill as defined but still invite the BLP.

Mr. CLERK: Just for clarity, this went as wide as it did because when that Bill went before the Committee, it had not passed the House. There was only one (1) speech and then it went to all of these persons. The difference here is that, this Bill passed the House and the Committee can determine what it determines, but certainly the only thing that can go back to the House are amendments, so I am just letting you know.

Mr. CHAIRMAN: That does not change a thing. We have that list of persons.

Senator the Hon. L. E. NURSE: Mr. Chairman, just for clarification from the Clerk, you said that the only thing that goes back to the House would be amendments. Will there be no chance then for us to recommend additional or even delete of aspects of the Bill?

Mr. CLERK: We can treat that as an amendment too. Whenever the Report is done by the Committee….

Senator the Hon. L. E. NURSE: In other words, if we, during our deliberations as we come up with something which may right now be outside of the scope of the Bill, can that be something that could be recommended?

Mr. CLERK: If it is outside the scope, we would then have to rename the Bill, so you really cannot go outside of the scope of the Bill.

Mr. CHAIRMAN: Any other recommendations would cover what you just said. The public meetings, I added on "in-person" here for the Committee's consideration.

Mr. CLERK: Mr. Chairman, before you go further, have we finished with the list of persons we are specifically inviting? Remember, we are putting an advertisement in the newspaper to invite all persons so whoever sees the advertisement can attend but in addition to that, there are specific persons who we want to come. Have we finished that list of specific persons?

Mr. CHAIRMAN: Is there any other group or individual who Members would wish to be specifically invited? "***The Chase Files"***, I think, is from Stephanie Chase, as you said? Add Stephanie Chase.

Dr. R. O. SPRINGER: There were persons who were very outspoken when this legislation was passed in the Lower House. I know Stephanie was one and there were one or two others who spoke out on Social Media. If we can reach out to one, I think that we can source the others. It is a small community.

Mr. CHAIRMAN: As I said, when I went on I saw Cammie Holder; Peter Thompson; Neil Harper; Stephanie Chase and obviously the Democratic Labour Party. I did not see any others but I did not take an exhaustive look.

Dr. R. O. SPRINGER: For one, I am sure I saw Kemar Stuart and he is part of the DLP; both here and internationally he was talking about it. Even if he is invited as a member of the Democratic Labour Party, I think you should single out him because he is one who is very active on Social Media. He should be singled out and invited because Ronnie might opt to come but….

Mr. CLERK: Mr. Chairman, I think what you can do as well, because there were persons who commented on the Bill on our site, is to try to reach out to those.

Mr. CHAIRMAN: Okay, yes. At one stage somebody implied you all deliberately took down the site so that they could not comment anymore. There was that accusation which I saw but then you all put it back up. Do we have an in-person town hall meeting? As I said, from what I said, Mr. Clerk, the Social Justice Committee did not do that for those two Bills but do you all believe that we should give the public that opportunity to do so? One town hall meeting? I believe so, that was why I added that. One should be enough, right?

Dr. R. O. SPRINGER: I do not know if you want to limit it to one because if there are certain matters that come up at that first one that you may need to go back and then return. Where are going to have that one? Are you going to have that one in some centralised location? Are you going to have that one in The City and maybe one at, say, Alexandra School, for those in the rural parts? You may want to do more than one. I do not know if you should have town hall meetings, but based on the outcome of the first one, we then determine if you should have more, rather than a set number of town halls at this time.

We do not know what kind of discussion is going to be flagged up after we have our first meeting and if it is something that we can cover in one session or if we

will need multiple sessions. We should just say a town hall meeting and determine….

Asides

Mr. CLERK: Mr. Chairman, are you sure you want to do town hall meetings? I mean we will fully advertise it. Persons are free to come before the Committee. Town hall meetings are an additional expense.

Mr. CHAIRMAN: I would have asked you what Budget you have. The reality, Mr. Eastmond and believe you me, you are going to do all of that and at the end of the day, there will be somebody who will say, *"I was not given the opportunity to talk. I did not know about this. This is Government being autocratic and want to ram this thing down us. Undemocratic because they won all of the seats."* That is why I put that in. I would want to go with one for now and reserve the right for more. As Dr. Springer said, seeing how that one goes, if there a lot of people who come there would also have to be Zoom facility as well.

I am cognisant of the fact that you may not have a budget for the three or so that Dr. Springer may wish. Again, I am going by the draft - Rights of Persons with Disabilities Bill. In the first instance, I mean we had three; one in Christ Church; one in St. Michael and one up by The Alexandra School. When we came back we had another three.

Mr. CLERK: You also have to take into account the time in which we have to report.

Mr. CHAIRMAN: Ninety days, that is why I said one. Dr. Springer and I seem to think one. What do other Members think? A town hall meeting or that…?

SENATOR G. P. B. NICHOLLS: Mr. Chairman, forgive me if I do not agree with the town hall meeting. I think, let people come to Parliament. Let them come here. When you say town hall meeting, you mean like going to a school hall or something like that?

Mr. CHAIRMAN: Yes.

SENATOR G. P. B. NICHOLLS: I think that takes away from the importance and the dignity of the exercise because, as the Clerk has indicated, this is a matter that has passed through the House. It is a parliamentary process that is in place at the same time. While I am not averse to taking matters out to the people; this is a process that is a parliamentary process. I think that we should respect it as such. I know that we probably might reach more people if we go out into the community but it is still a parliamentary process and one of the processes that we are engaged in.

People should come whether it is here in the Senate Chamber, the Committee Room or wherever, to accommodate as many people as possible. You probably would want to limit the amount of people who can attend in-person for security and spatial considerations. This is an open Sitting of the Joint Select Standing Committee on Governance and Policy.

You do not see in mature societies the committee process of Parliament out in school halls, at a church hall, and that kind of thing. I am not saying that that is what you intend but I am just very conscious of the image and the very noble exercise of condescending to the public in your own space; pausing your deliberations in your own space, to take into consideration. I think that is as noble as you can get.

I would hope that the Government Information Service (GIS); **YouTube** or wherever we can go on Parliament's website with a public meeting of the Committee, as we are meeting.

Mr. CHAIRMAN: What I seem to be gleaning from what Senator Nicholls and Mr. Eastmond have said, is that there is a bit of a difference, in that we are not now looking to formulate a Bill and policy. You actually have legislation that passed the Lower House. There is that difference that if you are now looking to bring the Bill before Parliament, it would be in order to go to the public in town hall meetings as was done, like I said, with the draft - Rights of Persons with Disabilities Bill. Since this is actually before Parliament, you are saying that you want to exclude public meetings. Alright, I think that you are persuading me. Dr. Springer, let us take that out for now.

If during the process, we see a need, perhaps we can have one. Zoom: how did you do it with the Social Sector Committee?

Mr. CLERK: I think the Committee determined that you would allow Members to come in by Zoom, so that all of those Members who could not be here physically could still participate.

Mr. CHAIRMAN: Okay, I could agree with that. Live streaming on Parliament's website. Again, hearings that were conducted. Were they streamed?

Mr. CLERK: Once we are doing like what we are doing now, the preliminary stuff, we do not stream that. Once we start the actual hearing, the Committee is an open Committee and is open to the public.

Mr. CHAIRMAN: **YouTube** and GIS….

Mr. CLERK: **YouTube**. We can give GIS the link. If the Press wants a link, we can give them a link as well.

Mr. CHAIRMAN: Okay. The media here, again, we got that from the Social Sector agenda. Tell us exactly what. You said we would invite them specifically but….

Mr. CLERK: I think that was more in terms of when the Committee was meeting in terms of the media. Sir, that was more like the advertisements that would go in the newspaper alerting about the Committee's work.

Mr. CHAIRMAN: Okay. The advertisement would go in - if I remember how it was done with the Social Sector - it would list the names of the Members; it would give the Terms of Reference and invite the public by a certain date. Alright. We have 90 days from today. I am assuming it is from today to deliver a report. I know that is what came up in the Resolution. Right? Ninety days?

Mr. CLERK: When it was referenced to the Committee. We are already into our 90 days.

Mr. CHAIRMAN: When was this referenced to the Committee now?

Mr. CLERK: Sometime last month for sure. What we may have to do if we do not complete it within the stipulated timeframe, is probably ask for more time.

Mr. CHAIRMAN: Let us get the exact date. It was the 25th of March or something?

SENATOR G. P. B. NICHOLLS: Mr. Chairman, while we are waiting to get the public engaged, at some stage we need to go through it ourselves or are we waiting for that process to …. Remember, I keep stressing that this was a thing that was halted by us as a Parliament; I think that we can still get on with our work because it is going to take some time to set up the public engagement and stuff.

Mr. CHAIRMAN: I am just trying to see when the 90 days started and when it ends. What are you looking at? To see when the Senate named the Members and…

Senator G. P. B. NICHOLLS: That was two (2) weeks ago.

Mr. CHAIRMAN: The 14th of February, 2024.

Senator G. P. B. NICHOLLS: Well the Committees were only constituted only two weeks ago so it could not be when the debate was halted.

Mr. CHAIRMAN: It was not when the Resolution passed?

Mr. CLERK: No. The Bill was referred to the Committee. We obviously, when we are requesting more time, you indicate that the full constitution of the Committee did not occur until X time.

Senator G. P. B. NICHOLLS: So you will refer to Committee from the date it was referred, but the Committee was only constituted two weeks ago.

Mr. CLERK: Remember it is like a Joint Standing Committee and that Committee in whatever form it was at the time was constituted. There were several changes since then, so we will have to use that as a means for asking for the extension.

Mr. CHAIRMAN: The 90 days run from the 14th of February, 2024; so work out then when the 90 days is up.

Senator G. P. B. NICHOLLS: The 14th of May, 2024, at the very least.

Mr. CHAIRMAN: Roughly around mid-May; so you all will do that when it comes.

Mr. CLERK: As Senator Nicholls said, while we work on doing the advertisements, the Committee could meet and go through the Bill on our own.

Mr. CHAIRMAN: So we are going come to that part under **Any Other Business**; so we are finished with No. 3 essentially? Do we agree that the two Bills should be done together? That is what I propose as was debated in Parliament anyway. So we agree with that. The two Bills shall be taken together, given that the subject matter is linked.

Senator G. P. B. NICHOLLS: Mr. Chairman, I do not know. I mean we can debate them together but you cannot consider them together. How can you consider them together because there will be issues that we will discuss here that are not going to relate to the other Bill? I am just wondering if this is a matter of just a forum because I mean we still have to go through...In other words, if we discuss the one and not the other, is that accurate? No. There might be issues that need to be dealt with in either; so I think that I am not sure if I am communicating what I want to say clearly.

Mr. CHAIRMAN: But somebody who comes before the Committee can talk on either Bill. In other words, there is not going to be a separate hearing and say, well okay, we are dealing only with Cybercrime Bill so you cannot talk about Mutual Assistance to us.

Senator G. P. B. NICHOLLS: I like being tidy. I think that is for the convenience of Parliament. We take it as how the Bill is introduced, right; this work is time consuming but to allow the public to **flash…(inaudible)** and I doubt very much any person will be coming to speak on both Bills before us so I am just wondering if we are not creating an artificial distinction in our minds because we still have to, as a Committee, to report on both Bills. I do not think that a discussion on them both, constitutes what a Committee reporting back to Parliament says, that we have gone through both, if we just lumped them together. We have to go through them individually.

Mr. CHAIRMAN: Yes, okay. This is what I will do, but the hearings will still deal with both. In other words, it cannot be separate, at least I would not propose that they be separate, or to separate the two, but yes, we still have to consider…

Senator G. P. B. NICHOLLS: Mr. Chairman, I am not being troublesome but Dr. Springer sat in this Chamber before and I know that perhaps you are not used to a Parliamentary Opposition unless you were in that Parliamentary Opposition but there are Senators who take very careful note of everything in the legislation and I fear that; if we do that process and there is any comma; full stop; colon missing…

"*Hang him, not save him*" is a different thing if you put the comma after "*Hang him not, save him*". You know the old adage *hang him not, save him* but if we say *hang him, not save him, we* have two different meanings. The comma goes in a different place and the man goes to the gallows and there are Senators who make very valid contributions on these things; so I just want to make sure that we are going through the process properly so that we do not have to hear in here, the noise, because you cannot really fight back because the concerns are legitimate. We have to take it here; it is not a really comfortable place to be in.

Mr. CLERK: Mr. Chairman, I think we should go through them individually once, as a Committee. Obviously, I suspect most persons that come before the Committee will be talking about Cybercrime. This has been one of my concerns when we do Bills as a cognate debate. Most of the time, the mover refers to one Bill and not to both and yes, it is done for the convenience of Parliament but a lot of times, the second Bill is not addressed at all but we will do the Bills individually, but when persons...

Senator G. P. B. NICHOLLS: There is nothing cognate about them.

Mr. CHAIRMAN: We will consider the Bills separately but that the public coming here can speak on them together. That is the suggestion. Right, okay. Agreed? Okay yes, so No. 5, we have to set some timelines now right? Considering that 90 days expires the middle of next month but since we are already half way then into that 90 days, more than that; that we would know that we have to ask for an extension and who would we have to ask, the Senate, since it came from them?

What timelines are we putting that are reasonable and within the context of our time as well and the time for Parliament? When can you all get the letters out to the individuals and give them a time limit? So how does it go, you give them a timeframe within which to submit a written memorandum? How does it go?

Mr. CLERK: Persons are given the options either to send written submissions and if they send in a written submission, to indicate whether they would also want to...

Mr. CHAIRMAN: To expand on it, but you give them a timeframe if they send in a written submission by when they should send it in.

Mr. CLERK: Two weeks, Ms. Gibbons?

Mr. CHAIRMNAN: Yes, I was saying 14 days and if an individual wishes to make an oral presentation, you give them two weeks to respond, saying so?

Mr. CLERK: When they actually make the written submission, they can indicate at that time.

Mr. CHAIRMAN: But suppose an individual wanted to just come before the Committee.

Senator G. P. B. NICHOLLS: Mr. Chairman, I think we should be encouraging people to be a little more disciplined. I do not think this is the appropriate forum to allow people to engage in what we call "soap box" politics. This is a Bill before Parliament. If you want to make a contribution to something that is a raging controversy and you have something substantive to say, put it in writing and they can come and introduce it, but we should be very controlled, in the manner in which we … I really, having sat down through the Constitutional Reform Commission process, and to sit down with a straight face to hear some of the garbage you are going to hear; the incoherent things you are going to have to hear; you have to do it but I prefer on a matter that is going to engage us as a Parliamentary Joint Select Committee, you should at the very least put out something in writing and submit it beforehand and allow us to engage you on the things that we may need you to come and clarify, at the level of the public.

I am not trying to say that we should stop people from walking and coming in off the streets but that should be the exception and not the rule. It should be the very rarest of circumstances because, what is the benefit of us sitting down and hearing random submissions on substantive provisions of an Act? What are we going to do with that? That is just window-dressing.

If you are coming to the Committee to make a contribution about a challenge that you have with the Bill, produce that in writing and let us engage you, where you are time-slotted and we want you to address these two things that you were as clear in your written submission or something like that, but not for people to come and engage in soap box politics for the purpose of it. When you look at C-span and other things; the people who come to those congressional hearings do not come and just talk as they like. There is a process; there are rules. It is a very tightly controlled thing. It is not a free-for-all and trying to get some minutes of fame. I think we need to control that because if we do not, we run the risk of having to subject ourselves to a whole series and torrent of verbiage.

Mr. CHAIRMAN: Point taken. How did it go with the other Committee?

Mr. CLERK: Just for clarity. The persons that we are specifically inviting, those are the ones that we want to hear. Is that correct?

Senator G. P. B. NICHOLLS: Let us invite to make submissions and then let them know that there might be a possibility and in our choosing, we would choose the ones who we think, in our wisdom, we need to hear from so to give them a hearing the Committee would have some questions for them, rather than them coming to talk to us. Let us do it in a disciplined way.

Mr. CLERK: So they do not have a choice in determining whether, having made a written submission, they would then want to make an oral presentation? We do not want to give them that choice? We are not saying that you can just walk off of the street but if we are inviting specific persons based on comments that they would have made when the Bill was done; you may want to say, well come and make an oral presentation. If the person sends a written submission and then indicates a desire to come and make an oral presentation are we going to preclude that person?

Mr. CHAIRMAN: No, we would make provision for that.

Mr. CLERK: We are not going to allow persons to just walk off of the street to make oral presentations but if they have sent in written presentations and they want follow it up with oral …

Mr. CHAIRMAN: Yes. In the advertisement now, the public advertisement, how would that be phrased?

Senator G. P. B. NICHOLLS: Mr. Chairman, remember that this is a specialist area that we are talking about. Again, may I stress that this is legislation that is already on its way and has passed through the House of Assembly. I am just trying to dissuade us from having an open-ended public hearing session from which none of us would be able to get any real grist to the mill.

Invite the public generally and special interest groups and persons representing specific industry concerns. Invite them to make submissions and then we would have a public session in which the Committee engages them on their submissions. We can ask them some questions and they would be able to amplify their submissions but I say do it in a controlled way rather than let us say, sit down and have Art Edwards and all of the other people who do not know anything about cybercrime, but will just come and talk things that are not relevant to the discussion.

Mr. CLERK: I understand what you are saying, Senator Nicholls but what I want to find out is: Do we get the written submissions in and then based on what has been submitted to us, we then determine we want to hear from this person? That is what I want to know.

Mr. CHAIRMAN: With the Social Sector One, can someone walk off the street and say I …

Mr. CLERK: Nobody could walk off of the street. You ask them to send written submissions and, as I said, this process is slightly different in that we have already passed the Bill but in instances if we had just gone to Committee … there are some persons that you would, if they are indicating that they also want to make an oral presentation, they can do so. Let me just give you an idea of what has been...

Mr. CHAIRMAN: Is that an advertisement?

Mr. CLERK: Yes. Basically, we would indicate that the Bill, obviously, is available on Parliament's website and you could make comments there as well and in keeping with parliamentary practice the Committee, obviously, through this Press Release, invites and encourages the public, whether it is individuals; professional organisations; community based groups; official and unofficial bodies with special interests and generally, anyone who may assist with its work to submit a memorandum or another documents setting out their views and comments on the issue.

"The Committee also encourages those persons who may tender written submissions to indicate whether they would also want to appear in person before the Committee to give oral presentations of not more than 10 minutes.

The Committee also invites persons who want only to make an oral presentation to indicate such desire and interest to the Committee.

The Committee also invites persons of sound witness under the law, to attend its meetings and give evidence to help toward formulating a well-informed and balanced report on the subject."

I am not sure if we might use that one because as I said this Bill has already passed the House of Assembly. Those are the generally rules. You invite persons to make written submissions and if they want to then supplement what they have written, can come before the Committee to explain and if the Committee, having read the submission, feels that there are some issues that they may want them to …

Mr. CHAIRMAN: Point. The Committee also invites persons who want to make only an oral presentation to indicate beforehand such a desire and interest to the Committee.

Mr. CLERK: And then they are limited to 10 minutes.

Senator G. P. B. NICHOLLS: Or you can say a limited number of oral submissions will be made but you would have to indicate beforehand that you are coming to make an oral submission; so you can allocate time for the people.

Mr. CHAIRMAN: No more than 10 minutes.

Senator G. P. B. NICHOLLS: Ten minutes?

Mr. CLERK: Ten minutes, yes.

Senator G. P. B. NICHOLLS: You know that ten minutes may turn into 15 and 20 minutes.

Mr. CLERK: If we say ten minutes, we have to cut. We are keeping the time.

Senator G. P. B. NICHOLLS: You would have to get a trap door.

Mr. CHAIRMAN: So we will go with that. So we will get the advertisement out and that can go into this Sunday's **SUNDAY SUN** newspaper?

Mr. CLERK: Friday, **WEEKEND NATION** and the **SUNDAY SUN**.

Mr. CHAIRMAN: Do we put it in twice?

Mr. CLERK: Yes. What we do is the papers that we think would have the widest circulation …

Senator G. P. B. NICHOLLS: But is that the widest circulation now, Mr. Eastmond? Does Parliament have a Social Media presence?

Mr. CLERK: Well we do not. Once you have a Social Media page, you then have to engage somebody who would be on that Social Media page every single minute, checking it, otherwise, you would be amazed at the things, even comments on Bills, that do not get to go on the site because there is some monitoring process.

Mr. CHAIRMAN: The proposal is to do it twice? To put in two notices.

Mr. CLERK: If we are going with this weekend for sure, we will have probably Friday and Sunday. Ms. Gibbons, will you all use **Barbados Today**?

Madam DEPUTY CLERK: Yes.

Mr. CHAIRMAN: You will use both **The Nation** and **Barbados Today**?

Mr. CLERK: Yes. Would we also use **Loop News**?

Asides.

Mr. CLERK: Government Information Service (GIS) would then disseminate.

Mr. CHAIRMAN: Okay, so that then is a week gone; then they are giving people two weeks which is three; so in the meantime, we would do research ourselves. We would get material such as that which Senator Nicholls correctly mentioned and I am well aware that, the United Nations (UN) is trying to formulate a Convention now of its own by the end of this year. The UN has had about six sessions so far; three in Vienna and three in New York.

The last in New York was, I think, in February this year, the exact time when this Bill was being debated, the UN was meeting. Barbados, I do not believe, has made much representation. I know they were checking out why but I know Guyana and Jamaica have been at all six of the sessions. We can get their material and obviously, the Budapest Convention and then the meeting which the Attorney General referred to was here; when people from the European Union (EU) were invited and the Law Reform Commission's Chairman chaired the meeting at the Lloyd Erskine Sandiford Centre (LESC), I believe, in October, 2023. We would also get that material.

Mr. CLERK: There was also the debate in the Lower House, which we would try to get to Members by tomorrow.

Mr. CHAIRMAN: The other material such as the Convention and the meeting here at LESC, you would have to get that probably from the Attorney General's Chambers?

Mr. CLERK: They may have that too because when I had discussions with them, they had drafted a lot of those conventions.

Mr. CHAIRMAN: Yes, the Budapest Convention, *et cetera*.

Senator G. P. B. NICHOLLS: Mr. Chairman, it would be interesting to know why we are modelling legislation on a Convention that is likely to be overtaken by another Convention in the same year? Will we come back two years from now or next year and say, "*Alright, we need to amend the Act because our international legal commitments in relation to this United Nations Convention on Cybercrime?"* We are not even a signatory to the Budapest Convention.

Mr. CHAIRMAN: My understanding was that we needed to pass this Act to become a signatory.

Senator G. P. B. NICHOLLS: But it is a European Convention. In fact, it is a Convention designed to govern relationships between European States.

Mr. CHAIRMAN: Due to the fact that that was the only international Convention, we patterned after that.

Senator G. P. B. NICHOLLS: Correct. I think the important thing is to have the mutual legal assistance provisions subsist in existing law. I understand the legal framework and the necessity for it, so I am not knocking that but that Convention itself right now is under review and then there is an international Convention….

Mr. CHAIRMAN: …which Barbados, as a member of the UN can sign onto, perhaps even more easily than Budapest. That is why I am saying we need to get deliberations at the U.N. as well. We might have to go through the Ministry of Foreign Affairs for that, for them to go through the U.N. Commission; our representatives there. Would that be the process which you all would take?

Mr. CLERK: Yes.

Mr. CHAIRMAN: Also write the staff and Mr. Stephen Williams because he was involved. This is John Williams' son. He also gave evidence before the meeting in October, 2023 and he, I think, assisted the Attorney General's Chambers on this issue. I can give you his email address easily. Okay, is there **Any Other Business**? We are giving people two weeks. In terms of getting material, when would we propose the next meeting to be and what would it deal with? Based on the Social Sector process, what would be the next step?

Dr. R. O. SPRINGER: Would the submissions be in written format in terms of hard copy and posted in the mail or would it be by email and posted directly.

Mr. CHAIRMAN: I think the notice says how people should submit. What does it say? It says by email; by mail; on the Parliament website and so on. Yes, the 23rd of April, 2024. Would you want to meet before that again with all of the material? Next week sometime? If you all can

get the material to us, we can meet next week Wednesday or Thursday.

Senator G. P. B. NICHOLLS: Sir, I am travelling and I will return to the island on Wednesday next week. I will travel Thursday and come back on Wednesday.

Mr. CHAIRMAN: We can come back Thursday next week in the afternoon. Thursday, 18th of April, 2024 at 2:00 p.m. Okay, invite the Chief Parliamentary Counsel (CPC) to that meeting. What about Sir David for that meeting too? Alright, invite Sir David Simmons and the CPC to that meeting next week Thursday, 18th April, at 2:00 p.m. Add Stephen Williams to the list of invitees and I will send you his email address. No, not to that meeting. Sir David and the CPC to explain. Alright. What I am wondering, just for the record, Parliament had advertised for assistance and technical support to these Committees. What is the position with that?

Mr. CLERK: No decision has been taken.

Mr. CHAIRMAN: As yet. Alright. Okay, any other business? Anything else? Member of Parliament, Mr. Phillips? Member of Parliament, Dr. Springer? Senator Nicholls? Senator Nurse? We are good? Okay, so we adjourn at just before 4:00 p.m. until Thursday, 18th April, 2024. We have the Bills in the package and I am sure that we will also go on to do our individual research to prepare for next week Thursday.

ADJOURNMENT

On the motion of Senator G. P. B NICHOLLS seconded by Mr. P. R. PHILLIPS, Mr. CHAIRMAN adjourned the Joint Select Standing Committee meeting until Thursday, April 18, 2024, at 2:00 p.m. in the Senate Chamber.

2nd MEETING
JOINT SELECT COMMITTEE (STANDING)
ON
GOVERNANCE AND POLICY MATTERS
ON THE
CYBERCRIME BILL, 2024
AND THE
MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024

Monday April 22nd, 2024

PRESENT:

Mr. Edmund G. HINKSON, S.C., MP, LL.B. (Hons.), L.E.C., LL.M. (CHAIRMAN)
Dr. Romel O. SPRINGER, J.P., PH.D., (Deputy Chairman)
Senator The Hon. Lindell E. NURSE, F.C.A, F.C.C.A., R.C.S. (ENT)
Mr. Ralph A. THORNE, K.C., LL.B., L.E.C., Dip. Theology
Senator Ryan O. WALTERS, M.B.A.
Senator Gregory P. B. NICHOLLS, LL.B., MICArb.

ABSENT:
Mr. Peter R. PHILLIPS (Chairman of Committees) (MP)

ALSO IN ATTENDANCE:
Mr. Pedro EASTMOND, (Clerk of Parliament)
Ms. Beverley S. GIBBONS, (Deputy Clerk of Parliament)
Mr. Nigel JONES, (Deputy Clerk of Parliament)
Miss Suzanne HAMBLIN, (Journal Department of Parliament)
Ms. Rhea DRAKES, (Office of the Chief Parliamentary Counsel)

Call to Order

The Chairman called the meeting to order at 2:00 p.m.

Mr. CHAIRMAN: Good Afternoon, Sir David Simmons, distinguished former Attorney General of Barbados and a former Chief Justice. He is here in the capacity as Chairman of the Law Reform Commission (LRC) which would have had an input into the Cybercrime Bill. Welcome to the Honourable Leader of the Opposition and other Members of the Committee from both Chambers; the representative of the Chief Parliamentary Counsel, Ms. Rhea Drakes; the staff of Parliament. We are here at the second meeting of the Governance and Policy Committee to hear Sir David give his views on the Cybercrime Bill, as currently drafted.

We will first go into the Minutes of the preliminary meeting held on Monday, 08 April, 2024; two (2) Mondays ago. Any amendments, omissions and additions that any Member would wish to make on those Minutes. The Minutes would have been circulated prior to the meeting. We take them as being read. Mr. Clerk, I know I would have added some things that we had said during that meeting in terms of who to write. Specifically, it was the Barbados Bar Association (BBA). I know we said to write them.

Mr. R. A. THORNE: Mr. Chairman, not meaning to interrupt you while you are underway, but at first glance at the Minutes, would you permit me to explain my absence and the absence of Senator Walters on the last occasion? I was certainly out of the country. I am certain that Senator Walters was out of the country as well. If the Minutes could be amended to reflect that we were not deliberately absent and that there was a good reason. We were out of the country.

I am obliged to you.

Mr. CHAIRMAN: Okay. I know information had reached that Senator Walters was out but we were not so sure about you, Leader of the Opposition.

Mr. R. A. THORNE: Yes, I was definitely out.

Mr. CHAIRMAN: Okay. We will put that to reflect it.

Mr. R. A. THORNE: Thank you, Mr. Chairman.

Mr. CLERK: Mr. Chairman, I would suggest to the Leader of the Opposition that if he is going to be out of the country, he should indicate to the Committee ahead of time. As the Chairman was saying, we were aware of correspondence from Senator Walters. We only found out at the meeting, very informally, that you were out.

Mr. R. A. THORNE: Very well. I will comply. Thank you.

Mr. CHAIRMAN: Mr. Eastmond, as I said, the part that would be on page four (4), to add: letters of invitation were requested to be sent out. I think I had given you the additional list. I remember we said the Barbados Bar Association. We said also each of the media houses; the Caribbean Broadcasting Corporation (CBC); the Nation Publishing Company; Barbados Today and STARCOM Network. I recall that we said the Barbados Media Practitioners Association. You would recall, Mr. Eastmond, that I subsequently called and asked you whether these specific institutions have indeed been written.

Were they indeed written? Any member of staff could tell us.

Mr. CLERK: I am actually checking the transcript to see.

Mr. CHAIRMAN: No. I am sure I mentioned it. This is the recorded transcript?

Mr. CLERK: Mr. Chairman, I do not think we have written the Barbados Bar Association as yet.

Mr. CHAIRMAN: Ms. Gibbons was saying something. That is your note as well. I certainly recall that; so who was written out of that list that I named just now?

Mr. CLERK: The letters were prepared Mr. Chairman but the difficulty that we had last week and so far this week is that we did not have our Messenger.

Mr. CHAIRMAN: But you have email. Is there something that says that it has to be hand delivered?

Mr. CLERK: No, but we would then have to get the email addresses.

Mr. CHAIRMAN: No, but that is easy, Mr. Eastmond; that cannot be an excuse. That is easy. Everyone knows the **NATION** and **STARCOM, BARBADOS TODAY** and the Barbados Bar Association email addresses; so let's please get that out today because Friday is the deadline. None of these letters have gone off? Who have received letters?

Mr. CLERK: The letters that we do not have the emails for would not have gone off.

Mr. CHAIRMAN: So who out of this list; has everyone received letters out of the list on Pages three (3) and four (4)?

Mr. CLERK: They would not have received it. The list is here.

Mr. CHAIRMAN: Pardon? Just turn on the microphone.

Ms. Suzanne HAMBLIN: Emails would have gone out to the Democratic Labour Party (DLP); Barbados Labour Party (BLP); Niel Harper had already emailed his submission so that did not need to go out as well as **BARBADOS TODAY** and the **NATION**. There was no email address for **STARCOM Network** readily available and Mr. Stephen Williams, I had spoken to him previously and he had alerted us that he would submit his submission and subsequently he did which was circulated.

Mr. CHAIRMAN: So what about let us deal with this in two (2) installments. What about the people who we said are on this list here in the Minutes? Stephanie Chase; Cammie Holder; Peter Thompson; Marcia Weekes?

Ms. Suzanne HAMBLIN: I have no way of getting email addresses for them. Those are the persons who would have commented on the Parliament website and I asked for the IT Department to post a notice on the website, in addition to the Press Release.

Mr. CHAIRMAN: What about Bishop Joseph Atherley?

Ms. Suzanne HAMBLIN: His is there in the mail for the messenger to take out.

Mr. CHAIRMAN: No, but surely we have his email address. Come on.

Mr. CLERK: Chairman, we will get the email addresses and send the information.

Mr. CHAIRMAN: You cannot tell me that you do not have an email address for **STARCOM Network**. I could give you that today, right now or for the Barbados Bar Association. We have to do better than that.

Ms. Suzanne HAMBLIN: The Barbados BAR Association; the email went out for them as well.

Mr. CHAIRMAN: So out of the media houses, it is just **STARCOM** that has not gone out?

Ms. Suzanne HAMBLIN: Yes.

Mr. CHAIRMAN: And the Barbados Media Practitioners Association or by whatever name they call themselves?

Ms. Suzanne HAMBLIN: I tried to reach them. I noticed that Ryan Broome was the President but he is no longer at CBC. I left a message and no one got back to me in terms of, well sorry. Some person had gotten back to me and told me they had passed on the message and he would call me at the office. I have not heard from him as yet.

Mr. CHAIRMAN: Okay. What about CBC?

Ms. Suzanne HAMBLIN: That is there for the messenger to take out.

Mr. CHAIRMAN: Sorry?

Ms. Suzanne HAMBLIN: That one (1) is there for the messenger to take out.

Mr. CHAIRMAN: No, no. Please email.

Ms. Suzanne HAMBLIN: Again, I do not have an email address**.**

Mr. CHAIRMAN: Again, that is easy so I will give you that and make sure that goes off before the end of today. Okay?

Mr. R. A. THORNE: Mr. Chairman, would you like a cell number for Bishop Atherley so that you can …

Mr. CHAIRMAN: This Parliament. Bishop Atherley was in here up to two (2) years and four (4) months ago and surely they have a cell number.

Mr. R. A. THORNE: Right, so you can contact him.

Mr. CHAIRMAN: I have his email address too. You have a cell number still for Bishop Atherley? It has not changed. I mean I could understand CBC's email but you all have Bishop Atherley's email address so let us not make a big deal of it, alright. Let us get that out today. Okay any matters arising on Page two (2). Members Page three (3). Page four (4). Page five (5). Page six (6). If no matters are arising, can we get confirmation of the Minutes as amended. As I said with the list, Senator Nurse, Dr. Springer?

Dr. R. O. SPRINGER: Seconded.

Mr. CHAIRMAN: I would want to say that I received an excuse and personally I do not know about Parliament but Mr. Peter Philips, Member of Parliament asked to be excused. He is attending a funeral this afternoon. Matters arising from the Minutes. Any matters arising Members? We can say a matter arising, Sir David is with us this afternoon. We have received written submissions from Mr. Neil Harper and from Mr. Stephen Williams and we must decide during this meeting, if and when, we would hear both of them in their written submissions.

Ms. Suzanne HAMBLIN: Mr. Chairman, if I may. I would have submitted an email to you indicating that Mr. Neil Harper indicates that he is not in the jurisdiction and has requested that if he is asked to make a submission, that he can do so via **ZOOM**.

Mr. CHAIRMAN: Yes, right and yes I got that email.

Dr. R. O. SPRINGER: Mr. Chairman, I hope I have not lost my opportunity to speak to this matter but in the listing of persons that were identified two (2) weeks ago, I think we had mentioned Kemar Stuart as one (1) of the persons who was most vocal about certain aspects of the Cybercrime Bill; yet I do not see his name. I know he is a member of the DLP but I do not see him listed as one (1) of those persons that should be identified.

Mr. CHAIRMAN: Yes, you had mentioned him. Please add Mr. Kemar Stuart to the list; I am sure you can get his email address, so pass on that email address too. Senator Walters you can pass on his email address. If no further matters are arising, we move to item four (4): Considerations of the Cybercrime Bill and the Mutual Assistance in Criminal Matters (Amendment) Bill, 2024. We will take Sir David Simmons on this issue. We will invite the media present to come in.

Just for the record, I wish to announce that this is being streamed from here on with Sir David Simmons' presentation. Sir David Simmons, I invite you to make your presentation before the Committee.

Sir David SIMMONS: Thank you very much Mr. Chairman. Good afternoon, Members of the House, Members of the Senate and members of staff of Parliament. With me is Rhea Drakes of the Chief Parliamentary Counsel's Office, who is the officer with responsibility for drafting the Cyber Crime Bill and the amendment to the Mutual Assistance in Criminal Matters Act.

Sir, with your permission, I would like to begin with a quotation from the judgement of Mr. Justice Frank C. Persaud in the High Court of Trinidad and Tobago, on the 26th of October, 2015

in the case of Therese Ho vs Lendl Simmons the former West Indies cricketer. At paragraph 35 of the judgement, the judge said as follows, inter alia

"The impact of social media and its consequent effect on our individual and collective privacy has to be acknowledged and addressed. There is a tendency for persons to hide behind the perceived anonymity that comes from using a 'username' and/or a user profile while sitting behind a computer screen or when using a hand held device to engage in offensive, hurtful, divisive and destructive discourse. These persons may feel that they are empowered but their actions can infringe upon the rights of others with the aggrieved persons having no recourse."

At paragraph 36 of the judgement, in respect of online conversations he observed as follows, *"The impact upon an individual's privacy is tremendous and the absence of clear and cohesive legislation to protect our citizens' privacy and to punish those who violate the rights of others, can cause us to descend into a bottomless pit of anarchy. The time for legislative intervention is long overdue."*

In its editorial of the April 6th, 2024, the **SUNDAY SUN** wrote inter alia, "*truth be told, some regulation is needed in Barbados if only to 1. Protect our children from those who will wish to do them harm through sex, manipulation and violence; 2. Hold people accountable for what they say about others; 3. Shield consumers from unscrupulous business practices; 4. Protect our constitutional rights to privacy and the maintenance of people's good name. The internet is invaluable, but it does not provide an avenue to shout fire in a crowded place when there is no just cause*.

Sir, the Computer Misuse Act that is presently part of the statute of Barbados Cap. 124B, was enacted in 2005. That is about 18 years ago or roughly 19 years. I think it is accepted on all sides including persons who have held themselves out to be experts in this area, that this Computer Misuse Act is outdated, because the march of technology and the variety of computer systems have made it antiquated. Secondly, it is far too narrow in its scope to be an effective tool for the police and prosecutors to cope with contemporary criminals and the variety of cybercrimes that have spawned since 2005. Thirdly, as was acknowledged by one of the critiques of this Bill, at first prior to Minister Caddle speaking, the existing legislation itself is in need of substantial revision or repeal. For example, Section 14 of the Bill, which deals with malicious communications, this is all it says, *"Where a person uses computer to send a message, letter, electronic communication or article of any description that is, (a) indecent or obscene; (b) is or constitutes a threat; or (c) is menacing in character, and he intends to cause or is reckless as to whether he causes annoyance, inconvenience, distress or anxiety to the recipient or any other person to whom he intends it or its contents to be communicated, he is guilty of an offence and is liable on summary conviction to a fine of $10 000 or to imprisonment for a term of 12 months or to both."*

The Cyber Crime Bill, 2024 that is engaging the attention of this esteemed Committee, is not Barbados' legislative response to the plea of Justice Frank C. Persaud. On the other hand, it is really this Bill, it is really the legal measure adopted by the Government of Barbados to establish certain criminal offences under our domestic law, but using the articles of the Budapest Convention, which is here in two different languages, English being one, as the benchmark against which the Bill is to be tested for compliance with that Convention.

No, I am aware the Law Reform Commission on whose behalf I speak and on whose behalf I am here, in the light of certain public criticisms of the Bill, have authorised me to discuss the issues under various Heads, to determine whether there is any validity whatsoever in the criticisms that have appeared in the print media.

First, one is freedom of expression or freedom of speech under the constitution. The second one which I will address, refers to the provisions of the Bill which touch on the concern of freedom of speech. Thirdly, I will look at criticised aspects of the Bill, repeating them, and then fourthly, analysing those criticisms. Fifthly, I will read a summary of the Law Reform Commission's position, and finally, I will look at the terms of reference which were sent to me last week, your terms of reference that were circulated.

Beginning first with the Freedom of Speech under the Constitution, what I will have to say may be old hat to Mr. Thorne as a lawyer and the other lawyers here but I have to say it.

I will take my time and go through this, so that there is no doubt as to what the law is in this

country. Beginning first with Section 11 of the Constitution at Chapter III, it states:

"Whereas every person in Barbados is entitled to the fundamental rights and freedom of the individual, that is to say, the right whatever his race, place of origin, political opinions, colour, creed or sex but, subject to respect for the rights and freedoms of others and for the public interest to each and all of the following, namely-
(a) life, liberty and security of the person;
(b) protection for the privacy of his home and other property and from deprivation of property without compensation;
(c) the protection of the law; and
(d) freedom of conscience, of expression and of assembly and association,
the following provisions of this Chapter shall have effect for the purpose of affording protection to those rights and freedoms ***subject to such limitations*** *of that protection as are contained in those provisions,* ***being limitations designed to ensure*** *that the enjoyment of the said rights and freedoms by any individual does not prejudice the rights and freedoms of others or the public interest".*

That is the general statement about the fundamental rights and freedoms which the Caribbean Court of Justice has held is justifiable. In Sections 12 to 23, the individual rights are spelt out in detail. The one that concerns us this afternoon, in relation to the Bill before you, is Section 20. Section 20 deals with protecting freedom of expression. The way Sections 12 to 23 are constructed, what you have first in the first subsection of all of them is what I call the imperative right.

You have then in second subsection, subsection (2) a derogation; the circumstances of which you can derogate from that imperative that is set out in subsection (1). Therefore, subsection (1) states:

"Except with his own consent, no person shall be hindered in the enjoyment of his freedom of expression, and for the purposes of this section the said freedom includes the freedom to hold opinions without interference, freedom to receive ideas and information without interference, freedom to communicate ideas and information without interference and freedom from interference with his correspondence or other means of communication".

This is what I call the imperative. Now, subsection (2) which derogates from that sets out the test; the test for determining the constitutionality of any law. Hence, it is against Section 20(2) that this Bill must be measured to see whether it is constitutional or not. Subsection (2) provides as follows:

"Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision-
(a) that is reasonably required in the interests of defence, public safety, public order, public morality or public health; or …"

We will stop there for a minute. If the Bill is reasonably required in the interest of one of those that I mentioned, then you cannot say it is in contravention of subsection (1). The alternative is if the law in question makes provision for as follows:

(b) that is reasonably required for the purpose of ***protecting*** *the reputations, rights and freedoms of other persons or the private lives of persons concerned in legal proceedings, preventing the disclosure of information received in confidence, maintaining the authority and independence of the courts or regulating the administration or technical operation of telephony, telegraphy, posts, wireless broadcasting, television* ***or other means of communication*** *or regulating public exhibitions or public entertainments; or…".*

Hence, that is test set out to determine whether the Cybercrime Bill, 2024 is constitutional or not, or if any provision of it is unconstitutional. We will come to those in due course. Therefore, I think it is important for me to emphasize that what I read is clear in its intent that such limitations as they are on the imperative are designed "*to ensure that the enjoyment of the rights and freedoms by any individual does not prejudice the rights and freedoms of others or the public interest".*

In short, the right and freedom of expression is not absolute. It is subject to limitations. Now, we have to test the Bill against Section 20 (2) to

determine whether it imposes limitations in the interest of public morality, public order or for the purpose protecting reputations from defamation, and so on. Those provisions in the Bill which deal with freedom of expression, if we may look at them as we go along first, Clause 16 dealing with Child Pornography. This was formally Section 13 of the Computer Misuse Act.

Although the clause criminalises child pornography indulging by different means, it provides a defence in
sub-clause (2) if a defendant can prove that the "pornography was for a *bona fide* research, medical or law enforcement purpose". If you are charged and can bring yourself within one of those categories, you may have a defence if you indulge in child pornography. However, I would think it is a fairly heavy threshold to attain.
I will come back to look at the language of the clause in detail because, perhaps, in passing I better mention that if you see section or Clause 16 (1) as it is now before you, it states a person who intentionally or recklessly does a whole series of things.

Mr. R. A. THORNE: Sir David, are you taking questions as you go along? I just wanted some clarifications.

Sir David SIMMONS: I can. No problem. I can.

Mr. R. A. THORNE: I just wanted to ask you. I am looking at sub-clause (2); the defence.

Sir David SIMMONS: The defence?

Mr. R. A. THORNE: Yes. This *bona fide* research; that causes me some difficulty.

Sir David SIMMONS: It would because it is difficult to see how it is achievable.

Mr. R. A. THORNE: In terms of definition, what is *bona fide* research?

Sir David SIMMONS: Well, the defendant would have to convince the court that he had these pornographic things because he was writing some learned academic paper and if he could, I suppose, and let us say he was from an established university and it could be shown that it was with the approval of the university, that he was engaged in this research, the Convention allows for that sort of thing.

Mr. R. A. THORNE: Consistent then with what you are saying Sir David, I am wondering if the legislator may not wish to extend it in the way you have defined it.

Sir David SIMMONS: Well, that would be for the drafters to do and I am not a lawyer who says he cannot draft because I believe that words are vehicles of thought and a lawyer must be able to draft. Say what it means.

Mr. R. A. THORNE: Say what it means.

Sir David SIMMONS: Do a contract or you have a client who comes to you with a contract. What are you going to do? Tell him well I am not a drafter. You are going to give him the best possible legal advice you can so I am not a lawyer who believes that because you may not have been a draftsman properly trained like Ms. Drakes that you are not at the same time capable of drafting accurately.

Mr. R. A. THORNE: Thank you very much Sir David; I just felt that since it is a defence important as defences are, the draftsman probably needs to give a larger explanation consistent with what you have submitted. A recognised institution, a university, research centre, I think the draftsman may need to extend the definition rather than just say *bona fide* research. Anybody can claim *bona fide* research.

Sir David SIMMONS: You know there used to be a *bona fide* claim of right, but that is no more because there are so many variations of claim of right. It could arise in several different fact situations or fact matrices; but the drafters can look at that.

Mr. R. A. THORNE: Thank you, Sir David.

Senator the Hon. L. E. NURSE: A little follow up. I am not a social media person but you know I would take up my phone, open it on **Facebook** and I get all kind of things which in my view is bordering on pornographic and various other things; now I have not gone on any site and downloaded or anything but they are there; so how can we be protected in situations like this?

Sir David SIMMONS: If you are offended by it I would suggest you report the matter to the police. You are going to bring me to a point where I did not necessarily intend to come to at this stage but let me just tell you my own experience. I am not going to play this one because it is so disgusting and especially as this is being streamed. I am not putting this back out again. I had to report this to the police 20th of July 2022. I can pass it on and you can see if you like or I can show you privately after. It was an advertisement for an oral sex competition to be held in St. Philip and the nastiness was displayed large and loud for everybody to see. This was sent to me and I was so disgusted by it I sent it, as you will see, to the

police for them to follow up on it. I did not have any difficulty when I saw that I knew it was pornographic so as a citizen my next step is to report it to the police because I am an ordinary citizen, in fact some would say that I am irrelevant, but my thing is to report it to the police. Okay.

Senator the Hon. L. E. NURSE: So, in this case what you are saying the onus is going to be on the individual…

Sir. David SIMMONS: If you are offended by it and you think that it crosses the line I think you should take it a step further and report it to the police. It would not be considered public mischief, it would be a public good.

Mr. CHAIRMAN: Sir David, in your view on this same section, *bonafide* research and medical purposes, with the consent of parents can also be added, with parental consent for this to be achieved and to be a defence?

Sir David SIMMONS: I would prefer to defer to Chief Parliamentary Counsel for the reason that I think you may need to check what is in the Child Protection Legislation and the Child Justice Legislation before you take a definitive position on it. The three may have to be cross referenced to get a true picture.

Mr. R. A. THORNE: Chair, I do not think the parent can consent to a breach of the child's rights and a child has the right not to be a subject of pornography so parental consent.

Mr. CHAIRMAN: I meant within this context, not outside of this context. Within the context of the research and the medicals, and the law enforcement.

Mr. R. A. THORNE: It would be a dangerous thing to mention parental consent because you are already sacrificing the child and a lot of pornography against children is committed by parents some knowingly and some unwittingly.

Mr. CHAIRMAN: No, but practically speaking how would you get a child to be subject of *bona fide* research and for medical and law enforcement purposes, without the knowledge of the parent and for it to be legitimate in compliance still with this law and as part of the defence to a charge?

Mr. R. A. THORNE: I would think the researcher makes the judgement whether the parent consents or not the judgement has to be made by the researcher as to whether it is *bona fide* so I would feel safe leaving it with the researcher, as to the *bona fide* research, as to what he is doing in spite of the parent's feeling because as Sir David is suggesting, if you go to the parent you are opening up a whole new area which may be in other legislation.

Sir David SIMMONS: Oh, yes.

Dr. R. O. SPRINGER: There is a tremendous amount of, unless you are a historian, this is just along the same line of research. Unless you are a historian you may not necessarily know there is a tremendous amount of information out there in various libraries and universities where historic photographs of children dating back from periods of slavery and periods in between there, the early days of photography. In many cases that information is held by persons who might have been curators of various museums and archives and such like. That information is shared during the process of study but after that period that information is kept but for the purpose that information was first acquired it was through the process of research or through the process of study. It is historic and dates back 60 or 70 years. It may be of some ethnic group, some remote part of planning, so where the cultural differences are obvious and seeing those would have been obtained during the process of study... The study for that period has passed and you still have access to that information. I did my PhD ten years ago and I still have records of some of the footage from that period. That footage is now found on my computer. What happens in a situation like that?

Sir David SIMMONS: That was a *bona fide* research?

Dr. R. O. SPRINGER: It was, 10 years ago.

Sir David SIMMONS: You can prove it was part of your thesis or whatever. It is a valid defence. It does not mean that it has to be current, so long as you can show it was *bona fide* whenever you were engaged in it, it will be a perfect defence. There are laws and criminal law which use that phrase *bona fide* as a defence. I cannot remember all of them off-hand now.

Dr. R. O. SPRINGER: The first point I made about information being historic, being dated back 80 or 90 years ago, persons even out of their own curiosity, they are not attached to any university, but they might study various ethnic groups for their own interest.

Sir David SIMMONS: I could see a situation, you know in England in the last 10, 15 years a number of entertainers or deejays, disc jockeys, were found to have been involved in child

pornography while they were at the height of their popularity. Jimmy Saville, I think was one.

Now, if there is a researcher who comes along, and you could never tell why people would go for a PhD and what subject they would choose, somebody might say, look, I would like to find out what motivated DJs in the 60s and 70s to do this. Maybe five or six cases in England and maybe elsewhere in the States, and somebody chooses that niche for investigation, I think he has a case to say this is *bona fide* research once it is supported and so on. It is that if you use the images and so on that will be protected by that piece of legislation, that defence that is given by subsection two.

Child grooming is the next one at section 17. This is new. This was not in the original Computer Misuse Act, but it is one of the modalities of contemporary cybercrime that you will see in other legislation. However, I wish to emphasise at this stage and I will later on also, that you read these clauses and sections, they all say a person who intentionally or recklessly uses a computer system for whatever purpose is guilty. It is very important to understand that this legislation does not, does not create any absolute offences such as you may have in a regulatory system that looks at small crimes, like not having to bicycle light. Do they still have those licences? In my day they used to have those licences on the back in heart shape, but those are regulatory things, so do not worry too much if there is no *mens rea* in those types of offences. Those are offences of strict liability. This legislation does not contain any offence of strict liability. Every offence requires proof of *mens rea*. There is *actus reus* and there is mens rea, the act and the guilty mind that accompanies that act. Therefore, so when you see here a person who intentionally or recklessly use it, the Convention on Cybercrime itself in its article speaks all along of intentionally doing something. Those words in themselves give a defence. Alright, take any offence here, take that one that I showed just now and the person sent it to me, and before I could properly look at it and understand it, my finger hit forward and it went to Dr. Springer and he got offended, and he went to the police. My defence would be that it6 was a pure accident. I did not intentionally send it to him, it was an involuntary act, not directed at him at all. However, it went and I could not call it back. Hence, that is why it is important to understand that as we go through this Bill. Right through the Bill we have provided for defences within the definition as well as defences separate and apart, defences within by the use of words such as intentionally or recklessly or without authority. Those offences which relate to access to the computer, breaking into the computer or getting people's passwords, you might see the words without authority. That is that nobody gave you the authority to go into, all based on the Convention itself.

On child sexual abuse, that is another one that is a new one at Clause 18. Again, a person who intentionally or recklessly uses a computer system to meet a child for the purpose of engaging in sexual activity with the child or where a cohesion inducement force or threat is used, *et cetera*, it is all there. We have tried to make the language of this Act as simple and intelligible as possible. Now it is dressed up and has a lot of legalese to make it complicated for the public to understand.

Now the one that has given the greatest I suppose opportunity for comment, has been Section 19. However, in the meantime, let me just look at Section 20 (1) first - cyber bullying. The same thought again, a person who intentionally uses a computer system to publish, broadcast, or transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene, or of a menacing character, or causes such data to be so sent, for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety, or causes substantial emotional distress is guilty of an offence and liable to conviction, *et cetera*. These are newish offences, cybercrimes that have come into vogue in the last five years I would say, we were encouraged to be as current as possible with this legislation by the Council of Europe, who administered the Budapest Convention and keep that up to date. I will say something about them later, and the assistance that they have rendered us and Barbados in the preparation of this legislation.

I do not need to say anything about cyber terrorism, that speaks for itself. Clearly, if someone intentionally uses or accesses a computer system for the purpose of terrorism is guilty of an offence and is liable on conviction on indictment to imprisonment for a term of 25 years. That is nothing to be sneezed at.

It carries some heavy penalties, as I will discuss later. Now, I want to revert to Malicious Communications because, as I said, when I come

to analyse the criticisms they tended to focus on Clause 19(2) and 19(3). Clause 19 (1) states as follows:

"A person who intentionally or recklessly uses a computer system to publish, broadcast or transmit computer data that

(a) intimidates a person;

(b) or threatens to

i. use violence towards a person or a member of his family; or

ii. damage the property of a person or the property of his family,

is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of 7 years or to both".

Sub-clause (2) states as follows*:*

"A person who intentionally or recklessly uses a computer system

(a) to publish, broadcast or transmit data that includes private sexual photographs and videos without the consent of a person who appears in them, ***with intent****…."*

It is not just using. It continues as follows:

"with intent to humiliate, harass or cause substantial emotional distress to that person; or

(b) to send repeatedly to another person data that is obscene, vulgar, profane, lewd or indecent ***with intent*** *to humiliate or harass the other person to the detriment of that person's health, emotional well-being, self-esteem or reputation…."*

Words such as "emotional well-being", "self-esteem" and "reputation" are finding their way into contemporary legislation because misuse of computers and malicious communications have had all kinds of negative impacts on recipients and people who were targeted for the purpose of humiliation, ridicule or whatever. The law is there to reign in some of this conduct and behaviour without trampling on the right to free speech. You can speak freely but that does not mean you have the right to curse somebody beyond their burial ground by telling a bunch of lies on them and so on. It does not mean that you must humiliate or ridicule somebody.

If you do that, then you are mashing the crease and the umpire's finger has gone up; out!

Mr. R. A. THORNE: Sir David, I wanted to ask you, since you have had the benefit of the literature, how do the Europeans feel about this?

Sir David SIMMONS: Very strongly.

Mr. R. A. THORNE: You said you do not look at social media. I think Senator Nurse said the same. Social media every second of the day is about insulting, humiliating and embarrassing. How have the Europeans addressed that in their prescription?

Sir David SIMMONS: In the sternest of ways.

Mr. R. A. THORNE: Really?

Sir David SIMMONS: The most….

Mr. R. A. THORNE: You can quote social media and every page is an insult and humiliation. I mean you are talking about the victims' peculiar sensibilities but social media is riddled with it.

Sir David SIMMONS: Yes, it is.

Mr. R. A. THORNE: I am curious as to how the Europeans feel. Are they condemning it or giving some latitude to the writer?

Sir David SIMMONS: No. They are very tough.

Mr. R. A. THORNE: They are very strict?

Sir David SIMMONS: The toughest of all is Britain.

Mr. R. A. THORNE: Britain?

Sir David SIMMONS: Britain has just introduced and you may see it on your **Google**, something called online safety or an Online Communication Act, or something like that, last year. It has 126 sections. It is tough, tough, tough.

Mr. R. A. THORNE: They are charging people?

Sir David SIMMONS: Well, I get the **Times Newspaper** every day on my IPad but I have not seen that as yet. I saw when there was a heavy debate in Parliament about that Bill.

Mr. R. A. THORNE: Sir David, I would tell you that your generation knows about the middle-of-the-road cursing. That happens every five minutes on social media. Somebody starts a conversation, like the newspaper would put up something and people start cursing each other, and insulting each other.

Sir David SIMMONS: Yes. Yes.

Mr. R. A. THORNE: I assume that under this, they are committing an offence.

Sir David SIMMONS: Yes.

Mr. R. A. THORNE: They assume they are not going to get charged because it is so commonplace.

Sir David SIMMONS: I do not know. It depends. If somebody takes exception and umbrage at what was said about them….

Mr. R. A. THORNE: Like the old blackguard legislation?

Sir David SIMMONS: Well, you know we had that. It is still part of the law, I believe, the Highways Act.

Mr. R. A. THORNE: Yes.

Sir David SIMMONS: I wish the Ministry of Transport and Works would send and ask us to do something with that legislation. As the Law Reform Commission (LRC), we could certainly beef it up. However, there used to be a poor man's slander or defamation in Barbados. Cursing at the standpipe was one. Using abusive words at or near a highway is still in your legislation. Right. All of those things, we do not worry with them now but when I came back to the Bar in 1970 that is how some of us survived in the early days you know; those standpipe cases.

You got a couple of dollars to keep us going.

Mr. R. A. THORNE: Yes. Bobby Clarke.

Sir David SIMMONS: However, let us look at this because there have been criticisms which I will come to show that they are not merited. Sub-clause (3) is taking partly from the existing law and partly from what we have done is to abolish criminal libel that is in defamation Act CAP. 199, and transported some of it into here; sub-clause 19(3). Therefore, this now includes the phrase and let me read it first. It states as follows:

"A person who intentionally uses a computer system to disseminate any image or words, not caring whether they are true or false, and causes or is likely to cause or subject a person to ridicule, contempt or embarrassment, is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of seven years or to both."

Now, let me just show you the type thing it means by looking at another one on my phone here. A few weeks ago, there was a big controversy in Barbados concerning a tower that was erected by Digicel down in St. James. I suppose the bloggers and everybody had a field day. Social media must have been full of foolishness. The lady who heads up Digicel, so far as I am aware, is the wife of Minister Wilfred Abrahams. I know her as Natalie. I do not know what was her name before she married. On the April 14, this is what somebody called **Atpatsoodat189** sent out. It stated, "*She is David Simmons daughter. Corruption.*"

Now, she is not my daughter. Of course, my daughter is Lynn-Marie, as the Honourable Leader of the Opposition knows. That is something that was published on a computer system recklessly. They did not care whether what they were saying is true or false. They wanted to drive David Simmons' name in there and then, put corruption on it and accused the lady being my daughter. This is the kind of thing that this legislation deals with. If you tell me that this is bad legislation because you seek to protect people's reputations from viciousness, then I disagree with you and we will part company.

Now, as I will show when I come to the defence that is implicit in the use of the word 'intentionally' in the Section look at Clause 19 (5). They went to great lengths to say that*, "The defences of truth, comment, triviality, privilege whether absolute or qualified provided for under the Defamation Act shall extend to a prosecution under Sub-section 3."*

Just suppose I had gone and complained to the police that this person published this thing recklessly not caring whether it was true or false about me and he or she had a defence and they could resort to 5 to say, *"Man tell Simmons don't worry about dat, dah is trivial."* You could raise a defence on triviality. If it was true having said it you could say, "But it is true." And I will stand on that, go to court and prove that it is true and would get the birth certificate of the lady and show that on that birth certificate the father is David Simmons. That is how it could be done. You have the defences written into the law. We have not been unfair to anyone. We have been very generous. We put in the law what defences you can rely if God forbid are charged but I will show that in none of the commentaries by all of the people and I have the clippings here all of those who have written not one has drawn attention to Section 19 (5) to say but the people gave us defences. If they are true we can rely on that. Yes, Honourable Leader.

Mr. R. A. THORNE: Yes, Sir David may I suggest that legislation extends itself because these are civil defences.

Sir David SIMMONS: But they are given a criminal … Yes. Yes.

Mr. R. A. THORNE: A criminal context, but if you want to establish your defence are you doing it on a balance of probabilities? You must be if it is a civil.

Sir David SIMMONS: If it is a defence you only have to go on probability. A defendant…

Mr. R. A. THORNE: As opposed to proof beyond reasonable doubt?

Sir David SIMMONS: The defendant never has to prove beyond reasonable doubt. The prosecution must, am I wrong? I am right yes. The prosecution must prove beyond reasonable doubt in a criminal matter.

Mr. R. A. THORNE: In a criminal matter but here it is you are giving a civil defence in a criminal matter but the defender must establish his defence presumably on a balance … and a lower standard...

Sir David SIMMONS: … In a criminal case. You are right.

Mr. R. A. THORNE: So you are importing civil standards of proof into...

Sir David SIMMONS: … But giving you the defence and saying you do not have to reach that threshold absolute proof beyond reasonable doubt. As long as you raise it like any other criminal defence it will be good, and you will just rely on the language of the particular defence in CAP 199.

Mr. CHAIRMAN: Sir David, the question could be asked because Sub-section 5 extends this defence to prosecutors under Sub-section 3. Why not to those under Sub-section 1? For intimidation, not for threatening to use violence or damage to property. Why would it not extend to the defence of intimidation of a person?

Sir David SIMMONS: A defamation defence cannot extend to something like that. A defamation defence only extends to something that approximates to defamation; not intimidation but then…

Mr. CHAIRMAN: But then the definition here of intimidate, include a person, causing a person substantial emotional distress. It could not extend, and I am just playing Devil's Advocate here, of course. It could not extend to that definition.

Sir David SIMMONS: I think you would be stretching it. Shall I turn now to the criticisms? Okay. Thank you. I have summarised them but I have them all here and the clippings from the **NATION** newspaper. The first one was a 'Mr. Peter Thompson' on the 4th of February in the **NATION**. It said, "*Among other deficiencies Part 2 19. 1 …* I do not know what that means *imposes a fine of 70,000 and seven years' imprisonment for transmitting computer data that intimidates the person even if the data is completely factual and in the public interest. Furthermore, Part 2 21 criminalises speech that is deemed offensive and causes anxiety or emotional distress."*

And let me tackle that one first, 21. It is true "*criminalises speech that is deemed to be, transmits data that is offensive, pornographic, indecent, vulgar, profane, obscene or of a menacing character*" but it says a person who intentionally uses a computer system. It does not just criminalise it, it criminalises it if you do it intentionally and he talks about that vague language being deeply problematic and can be leveraged to prevent criticisms of politicians, public personalities, for political persecution. Well I would not comment on that.

The next one was Ms. Stephanie Chase on the 8th of February. She alleged that Freedom of expression is under threat from State and non-State entities criticising section 19 (1) and 21 as including vague language. The language that they are saying is vague is where we use words like, "pornographic, indecent, vulgar, profane, obscene or of a menacing character". Or in 21 (b) "for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred anxiety or substantial emotional distress.

Now tell me, first of all the interpretation of those words is a matter for the court but before you get to court you have to pass the police. I go back to the one that was published (regarding the Digicel matter wrongfully alleging someone to be his daughter). Now suppose I took that to the police. I would give my statement. The police officer is bound to ask me, "But how has this affected you?". It is just like when the Honourable Leader of the Opposition, when you are doing a 'threats case' you let the witness or the client give his evidence. However, one question you do not omit is when he told you those words that he is going to kill you, how did you feel? How did that affect you? Then the person will say, 'I was frightened, I was real frightened'. The magistrate will write that down. That is the evidence of the effect of the words on the person. Just here with my case, I go with this and show the police and

they ask me, how has that affected you. I will say first of all, it is setting me out to be a liar. Now all along I told my family I only have one daughter, but they gave me another one and I have been humiliated and the police will say, yes, I see your humiliation here. They will charge the offender for intentionally using … or whoever the person is that sent this one, that you used your computer on the 14th of April to write so and so about David Simmons and to humiliate him using the language under this Section. That is all they have to do, so that these words that they have called vague such as, indecent, vulgar, profane, obscene, embarrassing, insulting, injurious, humiliating, and so on, first of all there are all words that have been judicially decided and on which the courts have had over the years to opine and define and there are words which go to evidence and how the particular data or matter that was transmitted affected you as the person who was the recipient, or about whom it was sent. These are things that go to evidence. They are not vague. You will see when we come to look at other legislation that they are all there in other legislation. Also in Nigeria, Guyana, and Seychelles.

Then, there was Marcia Weekes on the 8th of February. She said, some Barbadians believe that the Bill would infringe on their constitutional rights, it is an "overreach". The Bill does not does not infringe on anybody's constitutional rights, in particular the right of freedom of speech as I have tried to explain. It is only where you do something intentionally or recklessly within the context of a particular sub-Section that and offence is committed.

Colville Mounsey on the 9th of February in the **NATION,** wrote an article in which he repeated the criticisms of those persons I mentioned, but not once, and this is my criticism of the Press, not once in an article, not a comment from somebody, but I think a newspaper has a duty if you were to write a whole page about some aspect of a Bill, you have a duty to set out the law as it exists. Not once did the **NATION** condescend upon a citation of the particular Section that was inveighed against, and I think that it is not fair. It had misled the public into believing that if you just publish something it has infringed your freedom of speech, although the law has said intentionally or recklessly. Twenty-three times in this Bill, 23 times that phrase intentionally or recklessly, or the word intentionally or the phrase "without right" is used to import a notion of *mens area*, mental element.

My former personal assistant, Mr. Caswell Franklyn on the 11th of February, he is quoted as saying to a crowd, "*with this Bill, you can be sent to jail if you say something which hurts someone's feelings, but if it is true, it cannot be defamation. Yet, this Bill is saying you can be prosecuted whether it is true or not which is contrary to our law."* All of that is wrong. I read the Section 19(3) about making a statement recklessly, not caring whether it is true or false. The word recklessly appears in the existing Computer Misuse Act. It is an offence, but it is where if you use a set of words recklessly but they are true and show you have a defence under Section 19(5), to show that the defence of truth presently exists in the Defamation Act.

Michael Ray (writer in the Press) was the most recent I had on the 15th of February, and I am not sure what to make of his article or letter, but he said there were an increasing number of social media users who are complaining about getting hacked. This deals with hacking: *(b) Unknown people are using names and images to send false and damaging information across space. True. (c) Persons are being threatened and blackmailed. True. (d) People are afraid to make online financial transactions for fear being hacked. True.* I am one of them. (e) *Computers are being used to transmit pornography. True. (f) Computers are being used to assassinate people's characters and make false accusations.* Again, true.

This is how he ends off his article having spoken so many truths. He calls for a Bill to be written in a way that, "protects thousands of sitting duck Bajans and protect vulnerable and innocent." Nice words. I am not sure what he is meaning, but this Bill I believe, protects all kinds of Bajans, high or low, if somebody uses the computer system to propagate nastiness about you.

Mr. Kemar Stuart, he said it is true, he was cited in an article on the 4th of February, he says it is true that if bloggers commit any offences by malicious communications they can be prosecuted. That is the existing law of Barbados. However, we have built upon that and expanded it, because in 16 years as I said earlier, the march of technology has been so swift and relentless that people have used computers and computer systems for all kinds of nefarious purposes. He

said, why should a Blogger wish to publish untruths about people and gain a reputation for disinformation. I cannot answer that. Not having analysed any sections of the Bill, he says it is unfair, untrue and almost blasphemous to suggest that users of social media would have little or no free speech. I will only ask Mr. Stuart to go and read the Sections as I have read them for him using the phrase "intentionally or recklessly" or where defences themselves are specifically created and written into the legislation. You will see it there now, Sir.

Mr. R. A. THORNE: Sir David, may I ask quickly?

Sir DAVID SIMMONS: Yes.

Mr. R. A. THORNE: Has any explanation been given for the severity of the penalties?

Sir DAVID SIMMONS: No. Would you like me to when I come to them….

Mr. CHAIRMAN: I was going to ask that question too.

Mr. R. A. THORNE: I will defer, Mr. Chairman.

Mr. CHAIRMAN: What is your feeling on the penalties and whether you feel they are too harsh. Not only on that Section but the penalties throughout the Bill.

Sir David SIMMONS: No. I have a matrix here.

Mr. R. A. THORNE: Sorry to interrupt you. You had not finished the 'criticisms', so I probably….

Sir DAVID SIMMONS: I was finished.

Mr. R. A. THORNE: Okay.

Sir David SIMMONS: Mr. Stuart was the last one.

Mr. R. A. THORNE: Like Mr. Chairman, I am very curious about it.

Sir David SIMMONS: Yes. I have a table of penalties.

Mr. R. A. THORNE: Yes. Thank you.

Sir David SIMMONS: Now, first of all, let us understand two things. The Law Reform Commission which prepared this Bill with the assistance, the direction and the sponsorship of the Council of Europe who supervised and superintend the Budapest Convention. We are only a recommending body. We do not implement. No Law Reform Commission anywhere in the world implements law. They may recommend introduction of a particular piece of legislation saying one thing or other. However, it is up to the Government when we send forward a Bill, to determine whether they are going to go with the penalties, as recommended, or feel free to change them.

The penalties in this Bill, fortunately or unfortunately, have not been tampered with by the Government. They are exactly as we sent them forward. In doing that, we had State Counsel assigned to the Commission, go through and do an analysis of legislation in this region where there is similar legislation to see if we are in the ballpark with those penalties which we recommend. I can say to you that the research and will let you have this because it is on the computer. I will let you have this. You can make copies or have me send it. It would be easier if I send it again as computer data and then, you copy it and circulate it to all of the Members.

This is on our computer. However, let me just run through and as I go through, you could make a note if you think it is too high or whatever. This is not for us to determine. All we did was to make sure we were, as I said, in the ballpark fully well-aligned with what other countries and in particular, Guyana is doing. Some of this legislation is close to Guyana because they are most recent. Some of the rest of the Caribbean is behind. Now, take Clause 4 first; Illegal Access.

Conviction on indictment; we are proposing $50,000 or imprisonment for five years or both. Guyana have imposed BDS$48,353. They speak in terms of millions, of course. They have GYD$5 million but when you boil it down, it is only BDS$48,000. We say $50,000 and they say $48,000. It is for you all to decide if that is too high.

Mr. CHAIRMAN: The imprisonment as the alternatives in the sections too?

Sir DAVID SIMMONS: Both of us go for five years.

Mr. CHAIRMAN: Okay.

Sir DAVID SIMMONS: Clause 5; Modification of programme or data. Well, this is a new offence. There is nothing really comparable. Jamaica does have something but, again, it is not comparable because Jamaica talks about first offence, second and subsequent offence, and we do not have that. However, they have in the case of a second or subsequent offence, regardless of if any damage is caused or not, a fine not exceeding JMD$5 million which is BDS$65, 169.44 of our money.

We are saying BDS$70,000. We are $6,000 higher. In Jamaica, I think, their legislation is

about 2015. Therefore, we are a lot more up-to-date. Clause 6; Interfering with programme or data. For conviction on indictment, we said $70,000 or seven years. Guyana has $77,365 because they speak of GYD$8 million or five years. Therefore, we are two years more and $7,000 less than Guyana. Interfering with a computer system, on indictment, is $70,000 or seven years. Again, Guyana is $77,365 or GYD$8 million. That was at Clause 7.

Mr. CHAIRMAN: How many years in Guyana?

Sir David SIMMONS: Five years. We say seven years.

Mr. R. A. THORNE: Of course, the penalties are maximums.

Sir David SIMMONS: Yes.

Mr. R. A. THORNE: Judicial discretion is not lost.

Sir David SIMMONS: No. It means liable to or up to. Illegal interception of data; $100,000 or 10 years, we say. This is a serious one. We do not have 'intercept legislation' but 'interception of data', and somebody hacking into your computer. It is GYD$8 million again or five years. We are substantially higher. We are about $23,000 more than Guyana in this one and five years more also. We may wish to change that. This one was Clause 8. Clause 9; Misuse of devices. It is $70,000 or seven years. Guyana is GYD$77,000 or five years. When I say Guyana is $77,000, that is the conversion into the Barbados equivalent. Clause 10 is $70,000 or seven years. This one we cannot work out very easily.

Guyana says in their Section 23, "four times the monetary value provided by that law" and of course, the same custodial sentence. Therefore, they are really not helpful. Jamaica, in relation to a second or subsequent offence, is BDS$65,194 or JMD$5 million, whereas we are saying BDS$70,000. It is a $5,000-difference there. As I said, we are eight years ahead of Jamaica. Their Act was 2015. Disclosure of access codes is $25,000 or years in Clause 11. Guyana is $29,000 or three years. They are $4,000 more than we are. On indictment, they are $77,000. On indictment, we are $70,000.

Now, Clause 12: Critical Information Infrastructure. This is very important. Having regard to the experience we had last year with the QEH when someone hacked their system we have written, with the help of the Council of Europe, this is really their definition, we referred the matter to them to get the latest and best definition of Critical Information Infrastructure; but I will advise the Government as early as now, to ensure that there is a protocol shared between departments which have critical information infrastructure, that we identify in Clause 12 … In fact, this is so important I will read it into the record now: Clause 12 "For the purposes of this Section, Critical Information Infrastructure System means, any computer system, programme or data that supports or performs a function that relates to:

a) electricity generation or distribution.

b) telecommunications

c) government services

d) emergency services

e) law enforcement, security or intelligence agencies

f) public works

g) any computer system, programme or data that may be designated as critical information infrastructure system by the Minister responsible for…"

And that is for the government to write in which particular Minister, and publish it in the Official Gazette. It is so vital that the incapacity or destruction of such computer systems programme or data would have a debilitating impact on the security, national economic security, national public health or safety or any combination of those matters in Barbados.

I am saying that I think the Government should look at those agencies which would be specified, and develop a protocol now so that in case one of them is hacked a whole set of actions follow, just as we have for hurricane preparedness and you bring in the private sector and you do all sorts of things. They need to do that because this business of hacking and critical infrastructure is not to be sneezed at. It is serious and internationalised nowadays, because at the end of the day somebody is hoping to get ransom out of it.

Mr. CHAIRMAN: Sir David, the categories of critical infrastructural systems or critical information infrastructure systems cannot be closed of course, so are we satisfied with the provision there that the Minister responsible for the Crime Prevention published in the Official

Gazette, any subsequent or subsequently thought systems that may be of national security importance, national economic security importance because of course the publication in the Official Gazette would therefore be by negative resolution, be laid in Parliament, just for the records for you to explain that process for the public.

Sir David SIMMONS: Does yours say the Minister responsible for Crime Prevention?

Mr. CHAIRMAN: The definition Minister in this Act?

Sir David SIMMONS: I do not think so. This one I think is something for the Chairperson of National Security. This is one for the Prime Minister to head any…

Mr. CHAIRMAN: Minister is not defined in the Act.

Sir David SIMMONS: No. That is why we left it. There is a blank space there that has to be filled in. They are two X's. Government needs to decide and I think this is so important that this is one that if you have a National Security Council or Committee this is the one should be responsible for that for implementing Clause 12. It touches National Security. It really is so important.

Mr. CHAIRMAN: But to add to it would be by way of negative Resolution in Parliament because this section…

Sir David SIMMONS: I am not sure. I am waiting on that. In fact, I am not sure that is something that should come to Parliament at all. I think the Government should have a policy that if the courts were hacked, so and so would happen, it would trigger a response from various agencies and we would take certain steps and certain actions. I cannot go into them, I am not a Member of the Government but it seems to me that that is how I would approach it and that was certainly our intent because this critical information infrastructure runs through all contemporary legislation and it is because the world recognises what is happening. The vagabonds who hack the internet and your computers and so on; getting at governments and banks and places like that; the private sector would have to be involved in this because they go after the banks as we have seen in Barbados. We have had that experience five or six times so I think that a policy could be fashioned between the public sector and the private sector as to how you would respond in a situation where there is a repeat like the QEH or elsewhere but I do not believe that it should go to Parliament. If it goes to Parliament you would defeat the purpose because the world then knows what you are going to do. Do not do it.

Now to look at some of the other clauses and penalties. Clause 14 - Computer Related Forgery we are 100,000 or 10 years on indictment. Guyana is $77,365 or five years. We are higher again by about $23,000 and certainly we have doubled the period of imprisonment from five to 10 years. Clause 15, Computer Related Fraud. This is new but Guyana has a similar provision $77,365. We say $100,000 or five years and then Guyana goes up to, sorry that was on Summary Conviction. On indictment they are $96,707 or 10 years. We are with them on the 10 years but our fine is $100,000. We are $4 000 more than Guyana.

Child pornography, Clause 196. On indictment we are $100,000 or 10 years or both. Guyana is $145,060 and imprisonment for 10 years or both. They are substantially higher for Child pornography. Child grooming and this is the same as for porn. Eight million dollars in Guyana which is $77,365. We are $100,000. They are five years and we are 10 years.

Mr. R. A. THORNE: Sir David, may I take you back to Child pornography please?

Sir David SIMMONS: Sure.

Mr. R. A. THORNE: The penalty, in the case of a corporation, was there any thought given to the director?

Sir David SIMMONS: Later on. The Bill has it in.

Mr. R. A. THORNE: Thank you.

Sir David SIMMONS: Online child sexual abuse $100,000, is the same as or pornography. Those are all kind of standardised. Malicious communication Section 19, we say $70,000 or seven years, Guyana says $96,000. Those that I was dealing with, reckless or intentional, dissemination of nasty material. I thought we had a provision in this for corporations, Ms Drakes, (*Office of the Chief Parliamentary Counsel*), do we? I thought we did.

Mr. CHAIRMAN: In fact Sir David, I was going to raise that as well, because Section 14 of the Jamaica 2015 Act as you have correctly stated the year speaks to that, that they have a separate provision for penalising body corporates which commit offences and penalise the director, manager, secretary or similar company officer, but my eyes did not see that reflected in this legislation.

Mr. R. A. THORNE: Mr. Chairman, what are the categories again?

Mr. CHAIRMAN: Extending to the director, manager, secretary or similar company officer, Section 14. It would be in your package.

Mr. R. A. THORNE: Okay. Thank you.

Mr. CHAIRMAN: Parliament gave us Guyana and Jamaica in the package. I think by email for our first meeting you will see that there, the Guyana and Jamaica legislation for comparison. Ours is closer to Guyana's, as Sir David has correctly said, because Guyana is more recent than Jamaica. However, Jamaica has that provision while Guyana does not have it.

Sir David SIMMONS. No, Guyana has it.

Mr. CHAIRMAN: Guyana has it as well?

Sir David SIMMONS: Yes.

Mr. CHAIRMAN: Okay.

Sir David SIMMONS: Guyana's legislation is 2018 and Section 21, Ms. Drakes, (*Office of the Chief Parliamentary Counsel*) make a note please. It says this: *"Where a body corporate commits an offence under this Act, the body corporate is liable to the fine applicable in respect of the offence;" (2) Where a body corporate commits and offence under this Act and the court is satisfied that a director, manager, secretary or other civil officer of that body corporate, (a) it consented or connived in the commission of the offence or; (b) failed to exercise due diligence to prevent the commission of the offence, that director, manager, secretary or other civil officer commits and offence. A person who commits an offence in subsection (2) is liable on summary conviction $5,000,000 or three years and on indictment $8,000,000 and five years."*

Sir David SIMMONS: I would recommend that we include that in our legislation, provision for corporate liability. I will leave that with Ms. Drakes to deal with.

Asides.

Sir David SIMMONS: Now referring to the response to the criticisms which seemed to focus on Section 19, particularly 19(2) and 19(3), the response of the Law Reform Commission is that the Bill satisfies Section 20(2) of the Constitution, because it is reasonably required in the interest of public morality, public order and also for the point of view of protecting people's reputation in defamation cases, and secondly the Bill cannot be unconstitutional to the extent that it requires *mens rea* for several offences and as I pointed out, there are 23 times when the phrase intentionally or recklessly or intentionally and sometimes without authority, is where that kind of phrase is used. It is a protection against arbitrary conduct being criminalised. That is where those people have written the newspaper have done a disservice to the people of this country, because they have not gone through the sections and analysed them. They just say it criminalises freedom of speech. That is not true at all. As I said, if a defendant can show that he did not act intentionally or recklessly, he has good defence on all of those charges.

Thirdly, in respect of Section 19(3), the Bill incorporates specific defences from the Defamation Act in Clause 19(5), one of the few Bills that has done that.

Fourthly, it does not threaten freedom of speech. What it does, is to emphasise to citizens who may use computer systems, that if they transmit data provided that it is not offensive in law or injured the feelings or repetition or other members of society, they can transmit their data freely. What can possibly be wrong with such a law that gives you freedom to transmit whatever, provide you do not curse people and abuse their families and tell lies on them and so on.

Now, the legislation replicates many similarities from other legislation as I said. We looked at Guyana and Jamaica, and Guyana is the best of those in this region. Then you have the United Kingdom and I can mention also Nigeria and the Seychelles. Just by looking at their arrangement of sections, for example Nigeria, part one deals with these objectives and application, part two, (1) protection of critical national information infrastructure, (2) designation of certain computer systems or networks is critical, (3) national information infrastructure, (4) audit and inspection of critical national information infrastructure. Part three, these were effects of penalties against critical national information infrastructure. Now these would become familiar with ours, unlawful access to computer, unlawful interception of communication, unauthorised modification of computer programme or data, system interference, misuse of devices, computer related forgery, computer related fraud, identity theft, child pornography and related offences. They have one called cyber stalking and

cybersquatting. Cyberterrorism, racist and xenophobic offences and corporate liability.

In Seychelles, similarly, unauthorised access to computer systems, access with criminal intent, unauthorized interception, unauthorised interference with computer data, unlawful possession of illegal devices, electronic fraud, system forgery, cyber extortion, cyber harassment, cyber stalking, offensive electronic communication, pornographic or obscene material, pornographic publication and so on. Most countries because of the way the Convention is written, just to give you an idea, take Article 4 of the Convention. It states as follows:

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law,

when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right."

Article 6 - misuse of devices; again this is a standard way of expressing it. It states as follows:

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right"

(a) the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;"

Our legislation is following faithfully the mandate given in the several Articles of the Convention. I go further. The Council of Europe last September sponsored at their expense at the Lloyd Erskine Sandiford Centre (LESC), a workshop to go through our legislation with us clause by clause. The first day was for judges and magistrates. The second day was for police prosecutors and the Director of Public Prosecution Office's (DPP). The third day, September 13, was for service providers. None of those participants criticised this legislation as being restrictive of freedom of speech. On the second day, we had as many as 46 persons attending from the police and DPP's office.

At the end of it all, the officials in Budapest congratulated us on what we had done as a Law Reform Commission and said that we now have in this Bill, the most contemporary and up-to-date legislation on cybercrime in the region. I want to say that you have to be careful in confusing notions of cybersecurity which is about systems, structures and so on. Cybercrimes are the ways in which criminals use cyberspace, particularly via computers to commit all kinds of crime.

SENATOR G. P. B. NICHOLLS: Good Evening. First of all, let me apologise for being late. I am not sure if we covered it but when I came in you were going through the various provisions. I am happy to hear you speak about the extent to which the freedom of speech is not unduly interfered with. My concern is with Clause 19 on Malicious Communications and whether in your view the draftsman has captured what you had in your mind as to behaviour that intimates a person. I say that against the backdrop of….

Sir David SIMMONS: That one on intimidation was taken from the Guyana legislation.

SENATOR G. P. B. NICHOLLS: The challenge that I have with that is that if you intimidated a person outside of using a computer, it is not a crime. There is some vagueness in the language that would require the interpretation of some policeman or an officer of the State to determine whether or not you are committing a crime because intimidation in of itself is not a criminal act. The language here is vague or could be susceptible to allegation that it is vague.

Therefore, it lends itself to being struck down in a similar way to how legislation has been struck down for lacking certainty. As recently as last year, the court, in my view rightly, struck down the old 19th Century legislation that created the offence of wandering.

Sir David SIMMONS: Oh yes**.**

SENATOR G. P. B. NICHOLLS: If a child was guilty of wandering, it was an offence. However, if an adult did it, it was not. Similarly, the case that comes to mind is the *McEwan and others v. the Attorney General of Guyana* case out of Guyana where the CCJ laid down the principles about requirements of certainty in terms of legislation criminalising behaviour. Therefore, what would constitute an objective standard,

behaviour that is intimidating? What would be criminal about it?

While there may be a reason to criminalise malicious communications via the internet because of the pervasiveness of the use of the internet to do things, there are people who might use outrageous statements or propaganda, particularly when it comes to elections and so forth, to cast a view or colour the perceptions of people who might not have necessarily made up their minds one way or the other. When does it become intimidating? When does intimidating behaviour become a crime? I thought that this section perhaps was the one that I felt was problematic, in that, it did not sufficiently express in detail and particularise the extent to which a person can be intentionally reckless by way of a computer be intimidating someone.

If I tell someone that 'you look too fat and I put a joke or a meme', where does the crime occur? In the mind of the person who apprehends and considers that they have been intimidated? Or in the mind of an onlooker who is watching to see…is there an objective standard? To my mind, I am flagging it here as one that perhaps needs some kind of elaboration because I suspect that the Bill, if it passes in this form, this will not stand.

Sir David SIMMONS: Alright. Your concern is just with intimidation. Not with threats.

SENATOR G. P. B. NICHOLLS: Not with threats. We know what a threat is. At common law, we understand.

Sir David SIMMONS: However, we go further. The threat is violence towards a person or a member of his family.

SENATOR G. P. B. NICHOLLS: And that is particularised.

Sir David SIMMONS: You have no problem with that….

SENATOR G. P. B. NICHOLLS: No, that is particularised.

Sir David SIMMONS: Therefore, your concern is with Clause 19(1)(a) which states "intimidates a person".

SENATOR G. P. B. NICHOLLS: There are some very soft souls in the country who might be easily intimidated by a meme, robust language or a robust exchange.

Sir David SIMMONS: Therefore, you would want a deletion of Clause 19(1)(a) and Clause 19(4)(a) where intimidate is defined. I will ask….

SENATOR G. P. B. NICHOLLS: Perhaps, Sir David, for the purposes of sub-clause(1)….

Sir David SIMMONS: The word "intimidate" is defined.

SENATOR G. P. B. NICHOLLS: It is defined in Section (4).

Sir David SIMMONS: It is defined there. The question is whether you think that that is enough. That is what Guyana has in theirs too … and it seems to be okay. Intimidate has a definition, so I am not sure...

Senator G. P. B. NICHOLLS: I am guilty of not reading the full Section so I apologise. I do apologise but it is clear that it has a limited statutory definition here and not the dictionary meaning of intimidation.

Sir David SIMMONS: It has a specific definition in this that is limited as between sub-Sections 1 and 4.

Asides

Sir David SIMMONS: If you wish the CPC (Chief Parliamentary Counsel) to look at that...

Senator G. P. B. NICHOLLS: Just to make sure this is an exhaustive definition and that is the Parliamentary intent because it is clear here.

Mr. CHAIRMAN: Just for the record. Guyana's Section 19 is comparable to our Section 19 and both of those sections are more detailed to Jamaica's comparable one which is Section 9, but Guyana uses some different words. They use like 'obscene and constituting a threat and menacing in nature, annoyance, inconvenience, distressing, anxiety'; so there is a difference in some cases with the exact wording between the sections but they are similar in their aim.

Sir David SIMMONS: Mr. Chairman I do not think that there is any difficulty in asking Ms. Drakes...

Senator G. P. B. NICHOLLS: Sorry, when I go through it I want to be very clear so that to intimidate means to cause a person substantial emotional distress. I think that is where…

Sir David SIMMONS: The person would have to give evidence as to how that affected them and the court would then decide whether that is emotional distress or its overplaying it or not. It is a question of evidence.

Mr. R. A. THORNE: and the court determines it on an objective standard because they use the word *reasonable* in sub-Section 4.

Asides

Senator G. P. B. NICHOLLS: Right, but for Section 3 it does not say anything about *reasonable*. It says, *"To cause a person substantial emotional distress"*.

Sir David SIMMONS: It is whether the things are true or false then a consequence of that is that the person has likely caused the person to be subjected to ridicule, contempt or embarrassment.

Senator G. P. B. NICHOLLS: Sir David, I am glad you said that but I am not reading that this is only where the … that this is not the case where the statement or the interaction, is either true or false. In other words, if I put a caricature of someone, or let's say I blog and I am known to blog about cricket and I used to call a former West Indies captain by a certain name, and it brought me some kind of fame and notoriety because I did an interview once in India before a match…

Sir David SIMMONS This is Sub-section 3 you are focusing on.

Senator G. P. B. NICHOLLS: Yes. So I am just wondering if you were to call a person 'pig foot' and that was to cause him emotional distress. They are some people who,and especially sportspersons who…

Sir David SIMMONS: There was one famous guy who would play cricket in the BCL competition. He did not like you to call him a certain name which related to poultry but I will tell you….

Senator G. P. B. NICHOLLS: But when we look at Section 19(4)…

Sir David SIMMONS: No. Go to Section 19 (5). When you read 19 (3) you also have to read 19 (5) because 19 (5) gives you every defence that is known in the Defamation Act and is applicable here with 19 (3). That is why it is important to read the whole Bill. The only Bill that sets out specific definitions like that, you say if somebody charges you here as I gave the example of the person who said that Wilfred Abrahams' wife was my daughter and they alleged corruption and it was said recklessly. They did not care if it was true or not but just using their computer to … they just felt David Simmons is a nice name to lambaste. Say David Simmons and then put corruption behind it.

Mr. CHAIRMAN: Sir David …

Sir David SIMMONS: But, then the person could argue that is trivial. Sir David too 'thin-skinned' or it is true, or it is just fair comment.

Senator G. P. B. NICHOLLS: Right, and I am probing the extent to which lawyers can argue these things so that whereas…

Sir David SIMMONS: The Leader of the Opposition made a good point about those defences.

Senator G. P. B. NICHOLLS: The intimidation point is not known to defamation. Can it be that it is not available? Those defences are not available where someone is charged for intimidating. In other words, are the defences in sub-section 5…

Mr. CHAIRMAN: He raised that Senator before you came.

Senator G. P. B. NICHOLLS: Only in Sub-section 3. For intimidating language. Yes. So that is the challenge I have for the intimidating language because what is the…

Mr. R. A. THORNE: As Sir David said earlier, it is not of the nature of a defamation. A defamation defence…

Senator G. P. B. NICHOLLS: So what would be the defence if the intimidating language is true?

Sir David SIMMONS: If it is true then it may not be intimidatory.

Senator G. P. B. NICHOLLS: Sir David I am not sure if you understand. I will make myself clear because I can say something that is true that causes a person to be intimidated and with serious emotional distress. It is true.

Sir David SIMMONS: But you would not have a defence under the Act.

Mr. R. A. THORNE: You then go to the Mischief Rule.

Senator G. P. B. NICHOLLS: Who determines that, the judge?

Mr. R. A. THORNE: Yes, the judge and what mischief you are protected against. If you tell a man something and it is true, you cannot be intending to intimidate him. It is true, so the Mischief Rule would tell you that the truth should not intimidate.

Senator G. P. B. NICHOLLS: And that is clear from the legislation?

Mr. R. A. THORNE: Statutory Interpretation

Sir David SIMMONS: Yes, Statutory Interpretation. You are applying a rule. What was that mischief that the legislation was protecting against?

Mr. R. A. THORNE: Precisely who it is protecting against.

Senator G. P. B. NICHOLLS: I am not saying that this can derail the passage of the Bill but I am just saying that we, I am thinking that they are people who might necessarily be overly sensitive to being characterised and criticised or lampooned and this now might become the basis of them bringing private criminal actions.

Mr. R. A. THORNE: Private? This allows private?

Sir David SIMMONS: Mr. Chairman, with respect I suggest that the Committee should refer this for further consideration by CPC who is next to you. Let her look at it and compare with other Legislation as well. She may want to refine it. You have raised a point but I do not think we should flog a dead horse.

Senator G. P. B. NICHOLLS: No. I understand. I am just making sure that if we are going to create a Statutory Offence I am not comfortable that we can leave it to Statutory Interpretation and then the subjective opinion of the court to give somebody a defence under the Act.

Sir David SIMMONS: Cast your mind back to Lady Chatterley's lover when that was prosecuted under the Obscene Publication Acts in England in the late 50's or early 60's. It is the court that had to interpret whether it was obscene or not and the same thing here the court has to interpret. It is just like under our Highways Act. I think it is the Highways Act where you charge a person for using language, abusive language at or near or on a Highway, and the court has to determine whether the language is abusive or they are a couple of other words in there. I cannot remember all of them, in Section 44 or something. The court has to determine the nature of the conduct or the language in this case to see whether it fits the definition of abusive or indecent, usually abusive or indecent.

Senator G. P. B. NICHOLLS: I have confidence that if you were the judge that would be so because I well remember your decision in **Ramsay vs St. James Beach Hotel**, where she cussed her employer and I represented the employer at the time, and she used some very muscular language, and you said that it was the indecorous venting of the Barbadian spleen, we are a society of men and not of angels. It was an obscenity that she used, but at the same time it did not go to the root of the employment contract. However, would every judicial officer, and I can think of some that we have in the system now, interpret the legislation in a way that gives a person a defence, where the victim is saying that I have been seriously and emotionally scarred with this intimidating language, or this intimidation that I have seen on the computer, and it may be true.

Sir David SIMMONS: Yes, but it still has to go back to the key words in this section, the person intentionally or recklessly uses computer system to broadcast or transmit computer data that intimidates a person.

Senator G. P. B. NICHOLLS: Yes, and I want to expose him, I am going to expose him now, listen to me tomorrow at 7:00. I am intentionally exposing him, but it is still true. Therefore, I might feel that this exposé that is coming tomorrow is going to have an emotional distress. The police come at my door or somebody else's door and arrest them. Then, will they have a defence that is pliable under the legislation? I know it is a new area and would have hoped that if we did create this new statutory offence, that there will be some certainty in the scope of the defences available.

Mr. CHAIRMAN: Senator Nicholls, I raised this before you came and Sir David is suggesting that we can probably have the Parliamentary Counsel look to see if it is possible, because I have raised it with Sir David and he felt the defence could not extend to Section One.

Sir David SIMMONS: No, it does not, specifically it says 19(3) and 19(5).

Mr. CHAIRMAN: No, it does not, but whether if it is legally possible it can. I think that is what Senator is trying to say too, that if it is true that you know you should have a defence.

Senator G. P. B. NICHOLLS: Or, if it is trivial?

Mr. CHAIRMAN: Therefore, I think. Let us see if the Parliamentary Counsel can have a look at that, because I know that from reading the criticisms that is one of the issues that seem to be coming out, that public figures always interpret it as being a politician, will use that Section therefore to say, you have intimidated me even though it comes out that what you are saying comes out as true or trivial. Therefore, we can have Parliamentary Counsel look at it. I take your point Senator, because I was going to raise that case as well, **Ramsay vs The James Beach Hotel**, where Sir David as Chief Justice said this is normal Bajan language. I felt it was right, because if I recall, the lady was right in front the

woman and could have easily hit her if she wanted to, but did not proceed to hit her or anything like that. I think it was over her wages being worked out badly she felt. However, yet, Judge Clifford as he then was asked Judge Husbands in a very similar case, which was cited Ramsay, ruled the other way in a similar hotel case and said that fear had been established *et cetera*. Therefore, there are some things that you have to leave to judicial interpretation, but we have to look at that.

Mr. R. A. THORNE: Senator Nicholls, I know you are focusing on intimidation quite a lot, but if you go to Section 20(1)(b), there are several other offences created there which you may have been referring to several: annoyance, inconvenience, danger, obstruction *et cetera*. Hence, the prosecutor does not necessarily have to stay with intimidation. Look at Section 20(1)(b), there are several other offences created there.

Asides

Mr. R. A. THORNE: I think one would have an argument as to whether you should criminalise… Sir David, I expect that the public will come back at us and ask whether we should criminalise inconvenience, danger, embarrassment, insult, injury, humiliation, intimidation. Intimidation is mentioned there again.

Sir David SIMMONS: You all could take out which one you feel.

Mr. R. A. THORNE: It is wide. It is very wide. You almost cannot say anything.

Sir David SIMMONS: The existing legislation is very narrow.

Mr. R. A. THORNE: Yes.

Sir David SIMMONS: We looked elsewhere to get some more width for that particular section. Take Nigeria for example, cyberstalking, any person who by means of a public electronic communication network, persistently sends a message or other matter that, (a) is grossly offensive or offensive or of an indecent obscene or menacing character or causes any such message or matters to be so sent or; (b) he knows to be false for the purpose of causing annoyance inconvenience or needless anxiety to another or causes such a message to be sent.

Senator G. P. B. NICHOLLS: What happens to the satirist and comic? I mean I do not know if anyone watches Jonathan Pie, but he is one of my favorite British political commentators, but he does it in a satirical way. You can go on **YouTube** and watch Jonathan Pie if you are not overly sensitive to profanities, but he explains the rise of people like Donald Trump in a way that may appear comic. What happens to that kind of speech in society and I am also very conscious of the Bill that was passed recently in Scotland that is now started a lot of criticism, so that as the Leader of the Opposition has indicated, how wide, because using the language outside of context of a computer assisted device is not a crime, but using it over the Internet becomes a crime. That is one of the difficult questions that we have to answer in putting this forward, because yes this is a whole comprehensive regime under the Budapest Convention, but is it that the criminal act is now being perpetuated with the use of the computer device, or is it because it is the used by a computer device it now becomes a criminal act? I think we need to be very clear with the distinction between the two, because if I can annoy somebody and embarrass them and humiliate them without the use of a computer and I can do it lawfully, why doing by means of a computer makes it unlawful.

Mr. R. A. THORNE: This is because the computer is instant and wide dissemination and you send it to China. What I wanted to ask Sir David without interrupting you Senator. Who is enforcing this? Which country is now enforcing this legislation?

Sir David SIMM0NS: All 69 countries.

Mr. R. A. THORNE: Yes, but is there any country in which people have been charged, repeated or courts have riddled with these kinds of cases.

Sir David SIMMONS: I saw one recently where somebody was charged in Guyana and got off.

Mr. R. A. THORNE: Guyana?

Sir David SIMMONS: Yes, not necessarily this Section, but under their legislation.

Mr. CHAIRMAN: That is correct. In Guyana they have cases.

Sir David SIMMONS: However, we are all familiar as Barbadian men with the scenario where a man has become careless in the management of his amorous relationships. He strikes up a relationship with a woman who is not his wife.

That third party then gets on the telephone six or nine months later on and calls up the wife,

"You think you got de ring, I got de man doh." All of that. If you are using that, doing it repeatedly and tormenting the poor woman, that happens in Barbados. We know that. I have heard of those things. Do you feel that should be allowed? Do you feel we should turn a blind eye to it?

Mr. CHAIRMAN: Even though it is true?

SENATOR G. P. B. NICHOLLS: Sir David, that is not the point. I do not want to delay the proceedings but we have a difference in society. When my grandmother died, who was my father's mother, the year I got married I was sitting in the church. Is this being recorded? Well, I can say it. My uncle was giving the eulogy and making the point that my aunt was born to another woman out of wedlock. My grandmother went to the house a few weeks later and asked for Georgie's child. I would not tell you what my wife said to me. Different thinking. Different society.

Mr. CLERK: Senator Nicholls, we are streaming as well.

SENATOR G. P. B. NICHOLLS: Yes. I am not speaking about me now but I am just saying that we live in a different society and in a different era. Yes, this thing goes all over the world. However, should not your appreciation or own acceptance of criticism, whether it be satire, humour or whatever, could we perform a modern day Shakespeare play to contemporary circumstances using this legislation? Some of the things that Shakespeare would have said about people, certainly that be found humorous as students, to what extent is the artist protected from that? If it is put on the internet it is crime but if it is done publicly, it is not.

Sir David SIMMONS: You would have to look at the particular section where it may say if you do something with intent. There are sections that say that. I read something from the Convention itself which specified that. It depends on the purpose for which you disseminate the material.

Mr. R. A. THORNE: The other operative word is "cyber". Abuse of cyberspace.

Mr. CHAIRMAN: Sir David, you are speaking of criticism. One of the criticisms by an individual is that the Bill seeks to follow the Budapest Convention but that that Convention now is outdated in some way.

Sir David SIMMONS: Not true.

Mr. CHAIRMAN: I just want to state it for the record your opinion. As we know, because we have not mentioned it yet, the United Nations (UN) is as we speak looking at having a Convention on cybercrime. I know for a fact that some Caribbean countries such as Guyana and Jamaica have participated vigorously. Not Barbados as much. They are hoping to finalise crafting that Convention and bring it to the General Assembly, I believe, by October. What is your answer on that criticism of our proposed legislation that by following the Budapest Convention it has outlived its time?

Sir David SIMMONS: That was Harper. I think the Minister, Ms. Caddle, in the Other Place dealt effectively with his criticisms. I would not want to repeat anything she said then. I saw it on television one night and was amazed that this is the same man who five years ago was calling for Barbados to update its Computer Misuse legislation. When you do that with this legislation, now he criticises it. He says that this is out-of-date. I do not know about that at all. Our legislation is in harmony with the Convention. This is all I could tell you. I have not seen what the UN is doing, of course. I know that they are working on something but this is the one that is enforced now.

There are great benefits, of course, once we accede to that. The process of accession is very simple. It was explained to us at a special meeting that the Council of Europe had with the Attorney General and the Minister of Foreign Affairs and a gentleman from his Ministry setting out the steps. They are about six simple things on one page that could be done. In addition to that, one of the advantages of acceding to this Convention is that as soon but, in fact, you do not even have to wait but it is better.

As soon as you sign on, the police in Barbados have access to all the countries which are party to the Convention for the purpose of sharing information about cybercriminals. It is very important. It is very important from the point of view of international cooperation.

SENATOR G. P. B. NICHOLLS: Through you Mr. Chairman, Sir David I was following the debate on the UN Convention because when this first came to our attention for Parliament, I was not aware personally that it was the Budapest Convention that the legislation was based on, so I was immediately following and attracted to a number of the discussion points surrounding the debate at the UN. Indeed, the UN Convention

purports to go even further than this Convention has gone.

The criticisms that are surrounding seem to be more trying to say that it is a further incursion into the rights. However, there also on the other hand, had a lot of justifications as to why the Budapest Convention has been circumvented by the cybercriminals. Obviously, once you set the….

Sir David SIMMONS: …they will have to do a Protocol.

SENATOR G. P. B. NICHOLLS: You cannot move fast enough and the amount of money in cybercrime that is generated is billions and billions of dollars; more than the GDP of Barbados. People traffic in this kind of thing. Therefore, my question is, we would have to, if we accede to a UN Convention, come back and revisit.

Sir David SIMMONS: Depends when that Convention comes into force. You have one now in Budapest that I think 69 countries have signed on to. As soon as we pass this legislation with any amendments, it does not matter. This will enable us to accede to that Convention and get the benefits of the Convention, while I do not think the one in the UN is going to be finished in a hurry. You know how it is with Conventions and parties squabbling over words and all of that.

It will take years but with cybercrime as it is now such a threat, we may get it through in three years. I do not know but I do not think we should wait. Barbados

cannot afford to wait because the Act of 2005 is no use anymore. We need to update it. This is the update.

Mr. CHAIRMAN: Sir David, just for the record, I wanted to read in because you read the Guyana legislation on offences by body corporates. I wanted to read in to the records Jamaica's Section 14. It states as follows:

"For the avoidance of doubt, where a body corporate commits an offence under this Act, the body corporate shall be liable to the fine applicable in respect of the offence."

Section 14(2) reads as follows:

"Where a body corporate commits an offence under this Act and the court is satisfied that a director, manager, secretary or other similar officer of that body corporate connived in the commission of the offence, that director, manager, secretary or other similar officer shall; also liable to be proceeded against for the offence and punished accordingly…"

Mr. CHAIRMAN: Of that body corporate connived in the commission of the offense that direct a manager, secretary or other similar officer shall also be liable to be preceded against for the offence and punished accordingly or if they fail to exercise due diligence, same words as in Guyana, to prevent the commission of the offence that director, manager, secretary or other officer shall be liable on conviction or fine, imprisonment; so yes similar.

Sir David SIMMONS: Well you have agreed that we have the…

Mr. CHAIRMAN: …the Chief to look into that.

Sir David SIMMONS: Sir, I would like to finish on a response to the terms of reference which you circulated to me and I will go through them one by one. In respect to Paragraph 1. Not only does the Law Reform Commission answer this term of reference in the affirmative but so does the Council of Europe. Perhaps I should read the terms and provide the relevant answers:

- *1. "To inquire into and determine whether the Cybercrime Bill as drafted fulfills the expressed purposes to ensure compliance with the International Convention, global standards and best practices to counter Cybercrime and to ensure international cooperation in the combating of crime".*

Sir David SIMMONS: Our answer to that is 'yes'. Not only were we answering it in the affirmative but the Council of Europe which worked closely with the Law Reform Commission in drafting the Bills, and I spoke about the three--day seminar that they sponsored last September, and how they have proclaimed that our legislation is the best contemporary legislation in this region.

-

- 2. Secondly, *"to examine whether the Bill is drafted curtails citizen's fundamental rights and Freedom of Expression as against the protection of the reputation rights and freedoms of other persons or their private lives."*

Sir David SIMMONS: The answer to that is 'no'. The Bill does not curtail citizen's fundamental rights. It enhances the protection of reputations as envisage in the Constitution. That part that I read out in Section 12 Sub-Section 2 and as exists in the Defamation Act Cap 199.

– 3. Thirdly, *"to examine whether the Bill is drafted provides the necessary checks and balances, safeguards an independent oversight to protect citizen's human rights, liberties and privacy rights from potential abuses including from expansive law enforcement powers in order to prevent miscarriage of justice I do not under Term of Reference 3"*.

Sir David SIMMONS: The Bill does not safeguard or provide independent oversight to protect human rights. That is not the function of the Bill. It is not providing independent oversight. That is the function of various independent human rights NGO's. They are the watchdogs. The Bill does not do that.

4. "To examine whether the Bill that is drafted provides adequate protection to all of the specific categories of persons who may potentially be vulnerable to Cybercrime."

–

Sir David SIMMONS: As far as we can see it does provide adequate protection for the various categories of persons to whom the various Clauses are directed.

5. "*To examine whether any of the provisions of the Bill as drafted are vague, overly broad, arbitrary and or subjective and uncertain in its imposition of liability*."

Sir David SIMMONS: The Members of the Committee have raised two matters which are to be referred back to the Chief Parliamentary Counsel for further review but generally I think for the reasons which I have asked in my presentation and having regard to similar legislation elsewhere I cannot agree with the implication in Term f Reference Number 5.

–*6. "Whether the penalties imposed by the Bill are disproportionate or unreasonable in anyway."*

–

Sir David SIMMONS: This is one for the Committee. I did the matrix, the kind of table and and read out many of them into the record. I would also have said that the analysis that we did when we fashioned the penalties, as I was able to show that many of our penalties are in harmony with Guyana and one or two we are higher than they are and in other cases they are higher than we are; but that is a matter for the Committee. I explained at the outset the function of the Law Reform Commission is to draft the legislation and submit it not to implement as is if the Government feels you cannot live with this recommendation on the Commission the Government is free to change because our function is only recommendatory and not to implement; and the whistleblower, that does not apply because I think Government has separate Whistleblower Legislation that came last year.

"To consider whether the Bill could impede innovation in the technology sector and discourage investment and research in digital infrastructure."

Sir David SIMMONS: That one I cannot answer. I do not think that our Commission can answer. That is something for the people who are engaged in technology connected to Cybercrime and Cyber security to answer. I cannot answer. Now the Mutual Legal Assistance in Criminal Matters Amendment Bill. Since the middle 90's we had Mutual Assistance in Criminal Matters Legislation and by Treaty arrangement with America we also signed onto to Mutual Legal Assistance Treaties with America and that MLAC was signed when I was Attorney General sometime in the late 90's maybe '98 or '99. This Amendment to the existing Legislation which as I said goes back to the middle 90's as you would expect a lot of that may now be outdated and certainly it was very limited as to the role of the Central Authority. We have tried in this Legislation, to better provide for an exchange of information between Central Authorities here and overseas; and whereas the previous Legislation had a lacuna that left out countries except if they were in the Commonwealth, we have now said the Bill applies to all countries so we closed that gap. Those are my remarks and submissions. Thank You very much.

Mr. CHAIRMAN: Sir David. I just wanted to raise two or three other issues. There has been criticism that I have seen, that sections of the Bill

I think where they speak about the police, police involvement, law enforcement, constitute 'overreach'. We are all politicians constituting this Committee and you know what happens sometimes. A policeman, let's say, might have a woman and another man might like the woman too and he might want to trump up something on the man. Our legislation, unlike Guyana or Jamaica, does not speak towards only Gazetted officers being able to get search warrants for instance, it speaks to any police officer being able to go and get a search warrant, swearing on oath before a judicial officer and going and search a computer, cell phone, *et cetera*. Is this a valid criticism that the Bill should speak towards only Gazetted officers having such power?

Sir David SIMMONS: I am glad you raised that, because that is the difference between Section 23(1) and Section 23(3)(3). For example, Section 23(1) says, *"where a judge or magistrate is satisfied on information on oath given by a police officer that there are reasonable grounds for suspecting that on offense has been, is being or is about to be committed in any place, and that there is evidence that such an offence has been, is being or is about to be committed in that place, the magistrate may issue a warrant authorising any police officer to enter and search that place."* I think should be the judge or magistrate.

Mr. CHAIRMAN: That point was picked up. In fact, I raised that issue with the Attorney General when it was about to go to the Senate and he took that point so that the Senate would make that change. Yes, it would have to be magistrate or judge. We agree. Now in terms of the police officer, do you think it should be a police officer of higher rank?

Sir David SIMMONS: That is why I drew attention to Section 23, because we talk there about other **Gazetted officer**, you will see those words in bold and I am recommending that we standardise them, put that in Section 23(1), **Gazetted officer**. There was a feeling that Gazette officer is above the rank of inspector, and when they would trouble someone at that level with Section 23(1) offence. On the other hand, I do not think they are going to be that many that this would be become a burden for the Police Service, I would prefer to see Section 23(1) and Section 23(3) similarly, **Gazetted officer**.

Mr. CHAIRMAN: Then Section 11. Sir David, I would invite you to look at Section 11, **Disclosure of Access Code**, and I am wondering if Section 11(2) really and truly is sufficient enough that Section 11(1) can be eliminated.

Sir David SIMMONS: Yes, Section 11(2) incorporates (1), therefore, you could delete Section 11(1) and just leave Section 11(2).

Mr. CHAIRMAN: That is my view. The only thing is the penalties. Penalty in Section 11(2) is a lot more than the penalty in Section 11(1).

Sir David SIMMONS: Those could be changed. I understand the function of this Committee is to make recommendations for the parts of the Bill that may want a little tightening.

Mr. CHAIRMAN: To Ms. Drakes, the definition terrorism in cyber terrorism Section 21, I just wanted to make sure that it is coincidental with the definition of terrorism in our Anti-Terrorism Act Cap. 158.

Ms. RHEA DRAKES: That is correct, Sir. Subsection two provides for the purposes of this section terrorism has the meaning assigned to it in section three of the Anti-Terrorism Act Cap. 158.

Mr. CHAIRMAN: Just for that to be on the records. Do any other members have any other comments to raise? If not, Sir David has had a full three hours almost, with you. We thank you tremendously for your effort, your time, and your thoroughness in coming before us and giving your views. You may be required to come back as to any other points raised by any other persons may come before us and need to be addressed; we will be open to that possibility if required. Otherwise, Sir, we thank you. I believe we have some light refreshments in a room that you would have been familiar with for almost 30 years.

Sir David SIMMONS: Only 25 years, Sir.

Mr. CHAIRMAN: Twenty years including your Senate years? Including your two years, yes, because you were in the Senate from 1981 to 1985.

Sir David SIMMONS: I was here 1981 to 1985.

Mr. CHAIRMAN: Right, four years. That is why I thought it was almost 30 years all along. We invite you into that room for some light refreshments.

Sir David SIMMONS: That is very kind of you. Thank you all.

Mr. CLERK: Mr. Chairman, are we finished or we are breaking and joining Sir David?

Sir David SIMMONS: Yes, because three hours is a long time.

Mr. CHAIRMAN: I would only wish to say when next time we would meet …. We only have two submissions so far. We would certainly want to hear Mr. Neil Harper by zoom overseas and to set that date. Honourable Leader of the Opposition are you good for us to set a date?

Mr. R. A. THORNE: I am, Mr. Chairman.

Senator G. P. I. NICHOLLS: We will have to set that date in conjunction with him.

Mr. CHAIRMAN: I think we are going to set it.

Senator G. P. I. NICHOLLS: Should we not try to meet with him and the other gentleman on the same day?

Mr. CHAIRMAN: Have you looked at Mr. Williams?

Senator G. P. I. NICHOLLS: Yes, I read both.

Mr. CHAIRMAN: DO you think we should have Mr. Williams as well?

Senator G. P. I. NICHOLLS: Yes.

Mr. CHAIRMAN: Okay, I do not know, next week is a short week, of course Parliament is resuming tomorrow, so presumably it would resume on Tuesdays so that would be out. I believe the Senate would resume next week Wednesday. Sorry next week Wednesday is also a Bank Holiday, so I am thinking of Monday two weeks from now, which is May 6th. This will give Mr. Harper and whoever else time, because submissions close on Friday April 26th, so that is why we have to get this letter out today, and whoever else may decide to come. See you Monday May 6th at 2:00p.m. Is this a good date Mr. Thorne?

Mr. R. A. THORNE: I have a meeting with the CRC. That is not on May 6th, is it?

Asides

Mr. R. A. THORNE: We will go with it, Mr. Chairman.

Mr. CHAIRMAN: Therefore, we are adjourning until Monday, May 6th at 2:00p.m.

Mr. CLERK: Mr. Chairman, just before you adjourn, I think Senator Watson had written in relation to the Press Release that we had indicated that we should allow, especially for persons who live in the diaspora, to appear in person using the **Zoom** platform. This is something we did not take a decision on when we first me. Therefore, we just want the Committee to okay that.

Mr. CHAIRMAN: Agreed. How would we now give notice to…? I mean that would another publication in the newspaper inviting persons who live overseas to so do?

Mr. CLERK: We would just have to put an additional note. She had indicated also that we should widen the media when we publicise when next the Committee meets. We had said we were only going to put it on Parliament's website but she is saying that we should put in the print media as well regarding the dates the Committee will meet.

SENATOR G. P. B. NICHOLLS: Mr. Chairman, I read the e-mail from Senator Watson and I have no objection to that. The widest possible viewing by the public of these deliberations is what is the objective, so I would like to propose that we adopt that as our modus.

Mr. CHAIRMAN: Those two proposals by Senator Watson who, for the record, is what? Leader of the Opposition Business in the Senate? To be agreed on. This means therefore a notice in the newspaper to that effect? Both the **NATION** and **BARBADOS TODAY**? Where else? Will you put this on other news media as well?

Mr. CLERK: Normally, we will use the Government Information Service (GIS) and then GIS would disseminate.

Mr. CHAIRMAN: We will inform GIS as well to publicise. Okay. If no more business, we adjourn at Monday, May 6 at 2 o'clock.

ADJOURNMENT

On the motion of Senator G. P. B NICHOLLS seconded by SENATOR R. O. WALTERS, Mr. CHAIRMAN adjourned the Joint Select Standing Committee meeting until Monday, May 6, 2024 at 2:00 p.m. in the Senate Chamber.

3rd MEETING
JOINT SELECT COMMITTEE (STANDING)
ON
GOVERNANCE AND POLICY MATTERS
ON THE
CYBERCRIME BILL, 2024
AND THE
MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024

Monday May 6th, 2024

PRESENT:

Mr. Edmund G. HINKSON, S.C., MP, LL.B. (Hons.), L.E.C., LL.M. **(Chairman)**
Dr. Romel O. SPRINGER, J.P., MP., PH.D., **(Deputy Chairman)**
Mr. Peter R. PHILLIPS, MP
Mr. Ralph A. THORNE, K.C., LL.B., L.E.C., Dip. Theology
Senator The Hon. Lindell E. NURSE, F.C.A, F.C.C.A., R.C.S. (ENT)
Senator Ryan O. WALTERS, M.B.A.
Senator Gregory P. B. NICHOLLS, B.Sc. (Hons.), LL.B. (Hons.), LL.M., MCIArb.

ALSO IN ATTENDANCE:
Mr. Pedro EASTMOND, (Clerk of Parliament)
Miss Suzanne HAMBLIN, (Journal Department of Parliament)

ABSENT:
Ms. Rhea DRAKES, (Office of the Chief Parliamentary Counsel)

Presenters

Mr. Niel Harper, Cybersecurity Expert
Mr. Steven. A. Williams, Principal Consultant, Data Privacy and Management Advisory Services
Mr. Anthony Greene, General Manager, STARCOM Network
Rev. Dr. Ferdinand Nicholls
Mr. Kemar Stuart

Call to Order
The Chairman called the meeting to order at 2:15 p.m.

Mr. CHAIRMAN: Good afternoon everyone. Does everyone have the agenda? Everybody? The agenda is here set out. We will defer Minutes of the second meeting and consequently Matters Arising and proceed straight to oral presentations by Mr. Niel Harper, who I believe is online to give his oral presentation. Mr. Harper, can you hear me? Mr. Harper, can you hear us?

Mr. Niel HARPER: Yes, I can.

Mr. CHAIRMAN: Good afternoon, welcome to the Joint Select Committee on Governance and Policy Matters and you are the first presenter this afternoon, orally. We received your written submission on the Cybercrime Bill as presently drafted and you have asked to be able to give oral presentations which this meeting is about and this presentation.

We are allowing you Mr. Harper no more than 10 minutes for your presentation. You have already submitted a written presentation and I would wish to encourage you not to really repeat anything that you have said in your written presentation. All of us can read and have read it and to use your 10 minutes to expand on any points which you wish to expand on. We are very strict with this 10 minutes. After this 10 minutes, any Committee Member will be permitted to question or ask you to further expand or clarify on anything you have said or written. So, thank you. You are free. The floor is yours.

Mr. Niel HARPER: Okay, just allow me to share my screen. There have been a number of inputs in terms of public discourse; a number of inputs around the Cybercrime Bill contents and how the Bill as drafted, can result in the abuse of

the laws. Abuse from the perspective of suppression of public discourse; terms of violation of human rights, so I just want to start my presentation to present just a few headlines that show from around the world, what type of abuse of have occurred and these are headlines from the last 12-18 months.

As you can see, there have been issues with abuse of Cybercrime Laws in Jordan, Thailand, Pakistan, Egypt, Philippines, India, Senegal and a number of different locations and it ranges from targeting and victimisation of opponents of public officials. It ranges from digital rights and abuses in terms of internet shutdowns to prevent persons from expressing themselves or expressing discord or disagreement with the government. It ranges from attacks on individuals in terms of spyware, disproportionate mass surveillance of individuals so I just wanted to use this as a bit of the back drop for my discussion.

I had submitted a number of different comments and I discussed legal access and my perspective part in terms of illegal **access** is that there are a number of legitimate uses of so called access in terms of testers; researchers; activists; whistleblowers which actually service the public good, so I just want to be sure that you understand that specific impact.

Particularly a big concern is that we have a lack of trained **court** officials and we do not have a specialised **court.** Speaking of this in terms of specialized **court** for example, the UK the King's **Bench** Division on Technology which has specialist judges which are known as masters, who have special training to address and adjudicate these type of matters to make sure that innocent or well-meaning persons are not imprisoned.

If the particular section on modification of programmes or data. This is particularly important because it is misaligned. It is not present in the Budapest Convention; The Commonwealth Model on Cybercrime, The **Malabo** Convention or any other of the Cybercrime Model Laws. This is actually an outdated **term** and it also uses outdated language and it criminalizes a number of modern, productive use **cases** for modification of software and data processing, rather it be Artificial Intelligence (AI); free and open source software; open data policies and creative **are common** in terms of modifying and sharing data. Permission granted to modify and share data outside of the normal authority of the person who has created that programme or data.

This section particularly is an unnecessary section and my recommendation is that it should be removed. It can be addressed by Part 2 (6) which should actually be changed to "Interfering with Data" to better align with the Budapest Convention. Interfering with Programme or Data; that is Part 2 (6). This again uses outdated language and it should really focus on someone that is intentionally without authority and causes them harm. If something is temporary or not and does not cause them harm, it should not particularly be a crime.

Criminalizing minor acts, especially acts that do not have any harm in terms public, individual and corporate harm is unnecessarily criminalizing individuals. The same thing with Part 2 (7), Interfering with a Computer System. This is another particularly concerning section in terms of poor legislative drafting and it really does not address the true criminality which is really again focused on intention without authority and seriously hindering the functioning of a computer. Many of the laws including the Convention, focus of seriously hindering, serious harm to ensure that minor infractions are not criminalised.

Illegal interception of Data which is Part 2(8), I wanted to focus on this section because interception of public information and this is why I particularly talk about the lack of understanding of modern computer systems and data management because usually one of the foundation of data management is classification. Some data is classified as public sensitive; confidential; strictly confidential. If data is public, why should someone be charged for interception of data that is publicly available? I think that is a misnomer and you should really look at if the intention is dishonest, harmful and if it is the interception of non-public information.

Misuse of devices, I have mentioned this in my submission. I want to particularly refer to the Budapest Convention, which says that misuse of devices, illegal access, interfering with a system, all of these should not be interpreted as imposing criminality and not for the purpose of committing an offence where it is authorised testing or protection of a computer system. Where there is legitimate use to protect a computer system; to ensure a computer system is robust and resilient; these types of laws should not be used to criminalise those practices.

The critical information infrastructure section, which is Part 2(12), my concern with this section is that really and truly, this is unnecessary for a Cybercrime Bill. It has already been addressed in multiple different sections of the Bill. What you really need to do is to create a separate critical infrastructure protection legislation that focuses on obliging critical infrastructure protection providers to implement strong cyber security measures and making sure that you are monitoring and ensuring that those measures are in place. That goes a lot further, in terms of protecting our critical national infrastructure than a kind of symbolic section about critical infrastructure.

Mr. CHAIRMAN: Mr. Harper, I just wish to inform that you have two (2) more minutes.

Mr. Niel HARPER: Yes, I know I have two (2) more minutes. I want to also stop a bit just to reinforce. We have had a number of people submit for two (2) hours, five (5) hours of public submission and as an expert, an actual expert, you are restricting their submission to 10 minutes. I think that is a bit unfair. With that being said, malicious communications, again, this really focuses on criminalising to a large extent, which is just normal online discourse. Another key thing is that the Budapest Convention and other model laws do not address malicious communication.

Also, trying to treat the Cybercrime Bill with criminal defamation is very problematic because the European Court of Human Rights, the United Nations, several human rights organisations, as well as intergovernmental bodies maintain that criminal defamation laws are unjustifiable affront to human rights. Several progressive nations have actually removed criminal defamation laws from their books and the section on cyber bullying.

Adults are supposed to be resistant to hurtful words. If you look across progressive nations, cyber bullying laws focus on schools; children and adolescence. They do not focus on adults and when they do; they are particularly restricted to violent acts, sexual abuse and harassment.

Search and seizure, I have already mentioned all of these things in my submission. I just want to go the last part. We have a problem in Barbados with capacity and building. We do not have a national strategic cybercrime capacity building approach for training law enforcement; prosecutors; magistrates; and judges; in terms of making sure that they have continuous development and that they understand existing and emerging technology; how those technologies interact with the law and to ensure that they have the right knowledge and skillset that they can actually administer these types of cases when they do come in front of them. That being said, I will stop here and I will take any questions.

Mr. CHAIRMAN: Thank you, Mr. Harper. Do any Committee Members wish to raise any issues which Mr. Harper has presented in either his written or oral submissions?

Mr. Harper, in your written submission, you criticised Section 9(a) and 9(b); under misuse of devices. You can correct me if I am misunderstanding you but the Section speaks to *"for the purpose of committing and offence"*.

A person who intentionally or recklessly without authority. "For the purpose of committing and offence, and that is Section 9(a)(1) and Section 9(a)(2) is the same thing?" Would you not agree with me, if I were to argue that hence the use of this device for legitimate testing and protection of computer systems, would not come within the prohibited ambit of Section nine (9)? Obviously, if you are using it for legitimate purposes, as you have argued, comes within the criminality of that section, you would not be using it for the purpose of committing an offence.

Mr. Niel HARPER: Just to be clear here, an offence here is a very nebulous term; it is not properly defined in the Bill. In many places, what are offences again are normal interactions with human beings online. There are other legitimate uses in terms of accessing programmes. We are mixing software data; addressing or using computer systems without the permission of the authority of the person who created them or the person who is licensed to the software.

What exactly is an offence because you have defined a number of offences that in the real world are not actually offences. My position was that if you do not properly define an offence or if you do not train your magistrates and judges to understand what these actual offences are, then you run the risk of criminalising what is not an offence and fining or imprisoning someone unjustly.

Mr. CHAIRMAN: Mr. Harper, I would want to argue with you that we have separation of powers in Barbados as you know very well; separation of the judiciary from the legislative body and Parliament cannot go into detail and

define every single word in every single Act. There has to be a role for the judiciary and that is the judiciary's prerogative to say whether it is an offence or not. That is my argument, Sir. **I am thinking as a lawyer for over 40 years, there has to be a role for the judiciary in this.**

What I would agree with you, Sir, is that we need to ensure the judiciary is well trained in it. For example, as I understand it, in September, when there was a three-day seminar here which Sir David would have mentioned it here in his oral submissions the last time we met, the judiciary was invited as well. I think your stronger argument is that, yes, we have to ensure that the judiciary is well trained on this issue but to say that Parliament should usurp the role of the judiciary and tell the judiciary exactly what is the definition of offences, *et cetera*, in my opinion infringes and usurps on the independence of the judiciary which is a fundamental concept of our system of governance and laws.

Mr. Niel HARPER: My response to that is, first thing, a three-day workshop which I am very familiar with those workshops that are done by the Council of Europe; that is not training. That is not education; it is discourse on best practices and protecting human rights, *et cetera*, but that is not training. I have trained for cybercrime law; cybersecurity; privacy and other similar matters for the last 20 years. We ensured in our field that there is continuous education for 20 hours, 40 hours, 60 hours and 80 hours per year. It is continuous education to ensure that as technology shifts and you see emerging and new technologies which affect crime in different ways, that you stay in touch, and you better understand so that you can administer these laws again.

Yes, you are correct. They should be trained but also want to say this. I am not saying that the separation of powers should be usurped but if you look at again progress nations, they have explanatory notes; explaining in detail what are the crimes and how to understand the difference between acceptable use and criminal use. They have guidelines. They have White Papers. These are administered along with the laws to serve as guidelines, so magistrates and judges can better understand the subject to make sure they are administering the laws in the right way.

Mr. CHAIRMAN: Thank you, Mr. Harper. At least, you seem to have to conceded that in terms of the legislative provision, there is nothing wrong but obviously in terms of the administration now of the law, the Government and that is different from the legislature now has to try and ensure that there is proper training in terms of the administration of the law.

Mr. Niel HARPER: Just to be clear, my submission very clearly says that there should be training or some type of mode of training that makes sure that your magistrates and judges understand the law. There is nothing to concede because I think we are on the same page.

Mr. CHAIRMAN: In terms of your criticisms and comments on Clause 12, the categories of Critical Information Infrastructure System and I am reading your written submission to say that this should be dealt with in Regulations, as opposed to in a parent Act. This is a matter, I think, for the legislative drafters maybe to advise on. The categories of Critical Information Infrastructure Systems should not and cannot be closed. I think we all accept that in terms of evolving society and governance, just like how categories of negligence, a judge once said in case law, could never be closed. Categories of Critical Information Infrastructure Systems cannot be closed. It would be contemplated that subsequently this category would be widened. What is your comment on that?

Mr. Niel HARPER: To address that, I was very particular with my recommendation. If you look at the United States of America (USA); the European Union (EU); India; Bangladesh and other countries and I am very familiar with those countries because I have developed their capacity building. I have trained their judges; legislators; *et cetera*. They have what are called critical infrastructure legislation.

What that legislation outlines, in detail, what is critical infrastructure. It outlines what you need to have in place as a critical infrastructure provider in terms of cybersecurity requirements; computer security and incident response. It puts obligations by law on critical infrastructure providers that they protect their critical infrastructure of the nation. It also creates a Government department that their job is oversight of critical infrastructure providers to ensure that those strong cybersecurity measures are in place. What I am saying is, that goes further in protecting national infrastructure than criminalising unauthorised access to critical infrastructure.

The majority of the persons who are going to access your critical infrastructure and do the damage are not in Barbados. There are people in eastern Europe and North Korea. These are people who will obscure their locations and their identity online, so you cannot even bring those persons to justice. What I am saying is that instead of focusing on symbolic and useless clause, you should focus on implementing laws that actually protect your critical infrastructure.

Mr. CHAIRMAN: My final query to you, Mr. Harper, relates to Clause 11; Disclosure of Access Code, where you have been critical of this clause. It is certainly arguable. I want to concede that subclause one (1) and (2) of Clause 11 are duplicitous and that one (1) could perhaps eliminated, as you seem to be saying. Which one (1) would you eliminate, if given the choice?

Mr. Niel HARPER: It is not even a which one (1). I think that whole section is not a useful section; that is not present. If you look at any model law or treaty, that is not addressed because there are so many normal use cases and non-criminal use cases for disclosure of access codes. You usually share codes when administering systems; you use shared codes when you are doing encryption; you can use a number of different shared codes and sometimes it may be without formal authority.

It may be interpreted as reckless. At the end of the day, this is not treated as a cybercrime in the **Malabo** Convention and the Commonwealth Model on Cybercrime, as well as the Budapest Convention. This is not just addressed. I do not see a reason for this section.

Dr. R. O. SPRINGER: Mr. Harper, this is Dr. Romel Springer here. I read your written submission and I must admit that when I first read that bit in the legislation, it did flag up some concerns for me and I think I raised it here during our initial discussion; at least I intended to. You are saying that basically and I caught that when I came in and I heard your oral submission that criminalising trivial matters and this would almost and this would almost and that is me paraphrasing your words from what I understood you to be saying and this in a sense is a trivial matter and that they are many normal usages where persons may inadvertently disclose access codes, passwords and so on so forth but the legislation speaks to:

a) the reckless disclosure and

b) it also speaks to I guess disclosure or gaining access to these codes, passwords and so for unlawful gain.

They are using that to earn or to gain money unlawfully. I am assuming, in most cases, that is the reason why people engage in things and working in a Ministry where data is so critical and important, I cannot see a scenario where there is not a piece of legislation that looks specifically at situations where persons because of the clearance that they have in their jobs, in the areas that they work.

It may not necessarily be listed as critical. I do not if the licensing authority for example, is listed or seen as part of the critical infrastructure; it may very well be. There is a lot of important data that is stored or persons who work within that department has access to, that can be sold on the market. I believe that persons if given that level of clearance and engaged in any kind of unlawful, reckless disclosure of that information whether it be names; codes; passwords what have you, there should be something in the law that gives the authority some sort of recourse and if we were to remove this section altogether, I think, I mean, there are other ways that persons can be prosecuted but I think that this gives us more direct authority in terms of how we would treat to persons who engage in that type of behaviour or criminal activity. If you can speak to it using those types of scenarios that I just placed there on the table.

There are other situations where, I do not believe a person who because they work for me and have access to my password and to my computer or anything like that, that if they share that password or tell someone that password that I obviously would want to see that person being fined $25,000 or three (3) years in prison but I would want that there is some sort of legislation to protect me, from even the person thinking that they can share my information on instagram (IG) or any social media platform.

Mr. Niel HARPER: So just to be clear, you have a quite a number of sections that address that. You have illegal access; misuse of devices. You have interfering with a computer system. You have interfering with data. Part of my concern again is that they are a number of redundant sections in this Bill that serve no purpose except as to confuse Magistrates or Judges, especially the untrained ones.

Again, I want to circle back to this is not treated in any other law. This is actually a holdover from our Computer Misuse Act and if we are supposed to be upgrading The Computer Misuse Act, my interpretation would be that you would streamline the law and make sure it is better aligned with International Treaties especially when you are looking or you have expressed an intention to accede to the Convention or when the UN has finished the discussions on their Cybercrime Law which aligns very much with the Convention. Then you are going to end up not misaligned with International Treaty and international Laws so why are you not just at this point, when you have the opportunity, just remove a section that is not aligned with International Law and serve no purpose. It is already addressed by several other sections.

Mr. CHAIRMAN: Are there any other Members who would wish to engage, Mr. Harper? No? In which case, Mr. Harper, we thank you both for your written and your oral submissions. We can assure you that we will consider them with the authority and weight that they deserve to be considered. We thank you.

Mr. Neil HARPER: Much appreciated. Thank you as well.

Mr. CHAIRMAN: Next up, we have Mr. Stephen Williams who is here present with us, so Mr. Williams we invite you to come forward.

Asides.

Mr. CHAIRMAN: Good afternoon, Mr. Williams.

Mr. Steven A. WILLIAMS: Good afternoon Sir; Good afternoon Members of the Sub-Committee.

Mr. CHAIRMAN: You are here pursuant to your written submission to this Committee which is examining the Cybercrime Bill and the Mutual Assistance in Criminal Matters Amendment Bill both 2024 and you gave a written submission in your capacity as Consultant to the Cybercrime Bill and you could explain exactly what you mean by that and we have invited you to give an oral submission, of no more than 10 minutes on your written submission, so you need not repeat what you sent in your written submission. You could emphasize, clarify and expand but we have already read your written submission and after you are finished your 10 minutes max, we will open the floor to any Committee Member that wishes to engage you on either what you have written or what you said orally here today.

Mr. Steven. A. WILLIAMS: Thank You. Good afternoon Honourable Members of the Parliamentary Sub-committee. Thank you for granting me the privilege and it is indeed a privilege to speak to you today. I would also like to express my gratitude to the Chairperson of the Law Review Commission Sir David Simmons for selecting me as the IT Consultant to the Cybercrime Bill. I am honoured to contribute my perspective towards refining this essential legislation.

Approximately 12 years ago, I was the victim of malicious and defamatory lie, published on a then popular social media platform. It falsely accused me of being a drug dealer who stole money from the government. A blatant and disastrous lie because that platform and content creator was located outside the jurisdiction; coupled with the limited scope of the 2005 Computer Misuse Act, I had no legal recourse to seek justice for the defamation I endured.

This new Bill is a significant improvement because it incorporates international assistance in criminal matters; ensuring that no one can hide behind geographic locations to carry out malicious attacks. Unlike the 2005 Computer Misuse Act which was mostly confined to domestic crimes, the new Bill aligns with international conventions providing the framework for effective cross-border collaboration. As a former Member of the Board of Directors at the Transport Authority, I saw first-hand fraudulent documents submitted to the board falsely claiming to be authored by the then Chairman and granted permission for various licenses and clearances.

These documents which use computer technology to misrepresent the Board's actions, aimed to deceive and exploit the system with the inclusion of offences related to computer related fraud; the new Cybercrime Bill gives the police a strengthened tool to pursue individuals who engage in these activities. This empowers them to investigate and prosecute those who manipulate digital information, safeguarding the integrity of organisation processes.

The Cybercrime Bill represents a comprehensive effort to establish a legal framework that tackles from the threat of cybercrime itself; child exploitation to the misuse of digital devices. However, as with any forward-

looking legislation, concerns have arisen by various stakeholders, which I now turn my attention to, to give my perspective.

Illegal access provisions, with regards to the broad definition of legal access provisions, the idea that it is implicating cyber professionals and activists, the lynch pin and something I will consistently reiterate, is it up to the judiciary to discern between malicious intent and unauthorised actions, is not customary practice for civil professionals to illegally break into network or computer system without proper clearance. I will say again; it is not the actions of a cyber-professional to break into a computer system or network, without clearance.

Regarding activists, even actions performed with good intentions or altruistic goals have consequences. The Judiciary must determine the difference between those with malicious intent and those whose actions albeit well intentioned, could cause significant harm.

Critical information infrastructure systems (CIS). The scope of CIS should be dynamic and inclusive to address emerging digital services. Currently, the Bill focuses on public utilities and government functions, potentially minimising unfortunately, the critical sectors like food and chemical production facilities. It is crucial to promptly publish complimentary regulations that ensures regular updates to the CIS listings such that it incorporates evolving technology with artificial intelligence.

Using the term critical infrastructure systems instead of what is in the drafted Bill, which is the critical information infrastructure systems, broadens the scope to include both physical and digital systems such as transportation, energy and healthcare. This comprehensive terminology ensures that both physical and digital systems receive adequate protection, recognising that disruptions in one (1) can affect the other.

Moreover, it will help you encompass emerging technologies such as AI and internet of things. This adaptability would enable the Bill to effectively protect all sectors vital to national security and daily life, aligning with international frameworks that broadly include essential services and systems.

Malicious communication. Like the defamatory lies I experienced will require strong safeguard to protect potential victims from unfounded and warranted attacks. This includes maintaining firm measures against those who intentionally or recklessly use computer systems to intimidate, threaten violence or defame others. It is essential that these protections strike in careful balance ensuring that the Judiciary discerns between malicious intent and legitimate public discourse. This approach allows us to protect victims without stifling free speech; creating a digital environment where people can share opinions safely while deterring harmful behaviour.

Disclosure of access codes. Under Section 11 of the proposed Cybercrime Bill, disclosing a password, access code or other means of addressing your computer system without authority, could technically lead to legal consequences including imprisonment of up to three (3) years or a fine of $25,000. Whether sharing for example, a Netflix password with a third party would specifically lead to such penalties is a matter that requires careful interpretation.

Mr. R. A. THORNE: I beg your pardon, Mr. Chairman, through you, I know Mr. Williams has been given a time limit.

Mr. Steven A. WILLIAMS: Am I over that time Sir?

Mr. R. A. THORNE: No. We are losing a lot of the meaning as he rushes through. Through you, I would like to encourage Mr. Williams to slow down so that I will understand what he is saying. Do not rush through at the expense of us losing the meaning because I want to follow you.

Mr. Steven A. WILLIAMS: Okay.

Mr. R. A. THORNE: Mr. Chairman, through you, may I ask that Mr. Williams slow it down, do not worry about the 10 minutes; 15 minutes is not going to kill anybody.

Mr. CHAIRMAN: Valid point.

Senator G. P. B. NICHOLLS: Mr. Chairman, may I also suggest that if he has speaking notes and may want to share them with us after as well because me and Mr. Thorne may have lost something.

Mr. CHAIRMAN: Two valid points. You can make the speaking notes available but like I said you can expand and **adlib** on anything you are saying.

Mr. Steven A. WILLIAMS: Sorry, I can surely slow down on behalf of the panel. This Section 11 of the proposed Cybercrime Bill, disclosing a password, access code or other means of accessing the computer system without

authority could technically lead to legal consequences, including imprisonment of up to three (3) years or a fine. For example, sharing a Netflix password with a third party would specifically lead to such penalties is a matter that requires careful interpretation.

As a consultant, and upon reflection, I wonder if this provision would be more appropriate for corporate disclosure of passwords, rather than domestic sharing which could be seen as a civil matter. I leave the decision with the Honourable Members of this Committee. If it remains as law, it is essential that courts carefully weigh intent and harm to distinguish everyday behaviour from generally unauthorised or harmful activity.

In conclusion, I wish to leave the Committee three (3) points. Intent, it is the core of this legislation that rests on the concept of intent. Just like in life's purpose is judged by how it is used, so to should actions in cyberspace be evaluated by intent. Parliament defines what constitutes crime; the Judiciary determines whether such acts have occurred based on evidence on intent.

Symbiotic regulations. This new law relies heavily upon complimentary regulations that dynamically update the list of critical infrastructure services and establish criteria for those qualified to assist the Commissioner of Police with digital forensics. These regulations are urgently needed to supplement and give teeth to the legislation itself.

Password sharing. While sharing passwords for personal use may be considered unethical; whether it is a criminal or civil matter, deserves careful deliberation. My concern with this provision, in this current form, is that it criminalises everyday behaviour which could lead to situations of possible entrapment or abuse. Thank you for your time and attention on these points. I hope that the points will help shape your decision to strive to create an effective balance and fair cybercrime legislation.

Mr. CHAIRMAN: I thank you, Mr. Williams. I will now open to Committee Members to raise any issues with you, relating to what you have said; what you have written or to the Bill in general. Senator Nicholls.

Senator G. P. B. NICHOLLS: Thank you, Mr. Chairman. Through you to Mr. Williams, I was listening with intent to your presentation and I was making my own notes. You did make a comment that Mr. Harper made before and something that I believe that I shared in our inaugural meeting which is in terms of the executive's capacity and when I say executive, I mean the State to issue guidelines and regulations. Citizens must know when they are going to go out there to do their affairs, whether they are engaging in an activity that is unlawful and when there is uncertainty as to unlawfulness, that creates a legal problem because then whether somebody is acting unlawfully, then that becomes an arbitrary exercise, which where an objective to one.

Normally, we do not have state issuance of regulations and guidance as is in other countries around the world. In this cybercrime era, we see a lot of guidance being issued. In your view, what is our capacity to do so and which part of the executive? Is it a new arm to be created? Is this to be a specialized body to be created? Who should comprise that body? Should members of the public have access to it to lobby to help form and shape the regulatory content that comes out and to what extent is the prosecutorial discretion to be guided by these regulations and how do we as a legislative body, the ultimate maker of the law, reign in any excesses that may occur to any disadvantage of the public?

Thank you.

Mr. Steven A. WILLIAMS: Thank you, Senator. It is a very detailed and comprehensive question in terms of where do we go from here after the Bill is passed in whatever form. You are right and if it is any agreement with the previous presenter, is the fact that this Bill needs Regulations. How it is governed and executed is the $64 million question because right now, I mentioned areas such as those who would have capacity to assist the Commissioner of Police. We need Regulations to determine what those qualifications look like, in terms of the critical infrastructure list. That is something is always evolving.

Under the current proposed Bill, a list of services has been named. Under the international standards and framework, for example, NIST which international standard by the National Institute of Science and Technology out of the USA and for transportation, we now have electric buses, the possibility is there that with the right training, some person can attack electric buses because it is digital. If some person was to attack the electric bus grid, God forbid and disable the bus which can basically disrupt the everyday life of Barbadians.

To my mind, we need not just Regulations but we need an authority to basically assist the Minister in their actions. The way the Ministry is structured right now, it is not structured to be a proactive and research-based arm for evolving technological trends. Normally, the Ministries in previous years, to my knowledge, relied a lot on *ad hoc* input from the private sector. Yes, we need an Information Technology (IT) authority.

Senator G. P. B. NICHOLLS: Steven, I have known you to be an expert in this field, like Mr. Harper, for a long time. There is the view that discussion in cyberspace, online, is necessarily free and a public discourse but a lot of these platforms are not necessarily very public. They are very closed networks or owned by private individuals who would develop the algorithms and the various mechanisms to steer a debate in certain directions. The public believes that these are free, open networks and so forth. The one I might be participating in may not be the same one that you are participating in. You might not be access to the same information because it is generated based on a perception at what we might like to see.

How do perceive that we can properly regulate this environment? This is all the techniques, no offence intended, the domain of people who are techno-savvy in

these areas. For those of us who happen to like a good spy movie or the modern movies with all of the technologies and the investigations going on using cyber resources, how do we cope with this environment? The legislation is a first natural step. To what extent, after we pass the laws, are we necessarily going to be able to detect cybercrime and to be able to protect people from it?

Mr. Steven A. WILLIAMS: Thank you. I think that before we have that authority, we have to determine exactly what we want to do. For example, the police need additional resources. I met a wonderful chap in the Police Service that is a forensic specialist but they also need other arms of the Police Service. Truthfully, Barbados has had a very rough time accepting the transition into the digital era. Let us look at your point with how then do we go forward with, I do not want use the word "policing" but let us say, supporting, monitoring and building out capacity for governance in terms of this cyberspace and social media space.

Part of it comes down to and I like what Barbados has done over the past, concerning the Social Partnership. There is a role for Government to play. There is a role for the unions to play in terms of ensuring that citizens and the members of unions have representation on, for example, an authority to make sure their interests are served. More importantly, we do need civil society on a whole to participate. What I have seen consistently is that there are a few people who understand the problem and then, puts squarely the entire problem at Government's feet. I think that that is part of the problem because Government only has so many resources at its disposal but yet social media and social governance is everyone's problem.

I think that what Government can do is provide the framework and an authority for people to actually feed in those concerns to. I think that is the next logical step. How is that authority structured should be something that is desirous of consultation. I do believe that even if we do that, there is still limited governance, I guess because we are not owners of the platform. Here is a classic example. You would find that within recent times, if you put up a post, that is okay under the cultural sense of Barbadians that Facebook may find it offensive.

Certain words we use every day may not have the same cultural impact and significance as Facebook. These platforms have their own cultural norms or policing mechanisms that have nothing to do with Barbadians. There are then things that are Barbadian that are offensive to us that these platforms do not flag but yet we have no control over them because there is not a Barbadian or a central authority. Unless you become like China, have the great firewall of Barbados where the Government is policing everything that goes in and out which I do not ever want to see, then it is incumbent upon third parties, including the Government, to play an active role in ensuring that whatever law is passed, feeds back into a mechanism that governs the country digitally.

Mr. CHAIRMAN: Honourable Leader of the Opposition.

Mr. R. A. THORNE: Thank you, Mr. Chairman. Mr. Williams, I ask very short questions. I do not make a speech here, so I am going to ask you some very short questions. Do you see your purpose here as that of either supporting or opposing the Bill? Let me ask again. Do you consider that it is your purpose

here either to support the Bill or to oppose the Bill?

Mr. Steven A. WILLIAMS: I am here to support the best possible Bill that Parliament can craft on behalf of the Barbados public.

Mr. R. A. THORNE: I take it that that is a yes? You see your role as being here either to support the Bill or to oppose the Bill.

Mr. Steven A. WILLIAMS: I am not opposing any Cybercrime Bill.

Mr. R. A. THORNE: Precisely.

Mr. Steven A. WILLIAMS: Right.

Mr. R. A. THORNE: So, you are supporting it?

Mr. Steven A. WILLIAMS: Yes.

Mr. R. A. THORNE: Right. Now, were you a consultant prior to the drafting of this Bill?

Mr. Steven A. WILLIAMS: I was a Consultant to Sir David Simmons pertaining to the Bill. Yes.

Mr. R. A. THORNE: You would admit then that you come with a bias?

Mr. Steven A. WILLIAMS: I come with a perspective to….

Mr. R. A. THORNE: No. Were you a consultant towards the drafting of this Bill?

Mr. Steven A. WILLIAMS: Yes, Sir.

Mr. R. A. THORNE: May I suggest to you, that you are unlikely to oppose something to which you were a Consultant.

Mr. Steven A. WILLIAMS: I guess that is known to occur but….

Mr. R. A. THORNE: I beg your pardon.

Mr. Steven A. WILLIAMS: I guess that is known to occur.

Mr. R. A. THORNE: Yes. So, you are agreeing with me that you are unlikely to oppose something; the drafting of which you were consulted?

Mr. Steven A. WILLIAMS: But, I did not oppose the Bill. I….

Mr. R. A. THORNE: I know that you do not oppose it but I am asking a different question.

Mr. Steven A. WILLIAMS: Right

Mr. R. A. THORNE: Do you agree with me that you are unlikely to oppose something to which you were a Consultant?

Mr. Steven A. WILLIAMS: Fair.

Mr. R. A. THORNE: You agree with that?

Mr. Steven A. WILLIAMS: Fair.

Mr. R. A. THORNE: Alright. We have established that. So, you do support the Bill?

Mr. Steven A. WILLIAMS: Yes, Sir. Correct.

Mr. R. A. THORNE: We can make this short, you see.

Mr. Steven A. WILLIAMS: Okay.

Mr. R. A. THORNE: Now, I was reading your conclusion and one of the reasons I asked the Chairman to ask you to slow down was because I was losing a lot of the meaning and I wanted you to slow down. You wrote a conclusion here. I was trying to read it while you were speaking. Let me read the first two (2) lines for you. *"The effectiveness of the Barbados Cybercrime Bill hinges on the ability of the judiciary to discern the intent behind the actions of defendants in cybercrime cases."*

Now, if you read the other four (4) paragraphs coming after that, in your conclusions you do make repeated reference to the judiciary and you seem to be placing the responsibility on the Judiciary in its effort to interpret that which you assisted in drafting. Together with the Judiciary responsibility, do you consider that Parliament has a responsibility prior to Judicial intervention, do you consider that Parliament has a responsibility to do that which is just?

Mr. Steven. A. WILLIAMS: Of course, Sir.

Mr. R. A. THORNE: Thank you very much, Sir. Those are my questions.

Mr. Steven. A. WILLIAMS: Can I follow up on that Sir, if you do not mind.

Mr. R. A. THORNE: Yes. If the Chairman allows.

Mr. CHAIRMAN: Sure, Mr. Williams.

Mr. Steven. A. WILLIAMS: Sir, of course but in my humble opinion, it is Parliament's decision to determine what crime looks like.

Mr. R. A. THORNE: I see, so the question then is, do you consider that what as we agree you focused on the Judiciary but I have taken you to Parliament which acts before the Judiciary.

Mr. Steven. A. WILLIAMS: Correct. I understand that, Sir.

Mr. R. A. THORNE: Do you consider that Parliament in the drafting of this Bill has done its duty entirely in terms of promoting justice?

Mr. Steven. A. WILLIAMS: I think the draft of the Bill while I do agree it is not a perfect piece of legislation. It is not perfect and nothing will be perfect.

Mr. R. A. THORNE: No. No. No. You said it is not perfect. Do not worry about other things. You are saying that this Bill is not perfect.

Mr. Steven. A. WILLIAMS: No, it is not perfect.

Mr. R. A. THORNE: Okay and you are going on the record. You know this?

Mr. Steven. A. WILLIAMS: Yes, I understand. It is not perfect. In my record, I actually said for example, Critical Information Infrastructure Systems.

Mr. R. A. THORNE: So they are areas in this Bill that you think need improvement.

Mr. Steven. A. WILLIAMS: I mean it is a Sub-Committee. That is why we are here.

Mr. R. A. THORNE: Yes, so I am asking you a direct question. Are you saying that there are areas of this Bill that require improvement?

Mr. Steven. A. WILLIAMS: It is not perfect and just like I mentioned that area, I think that we would get to a more perfect Bill when we deliberate these sorts of discourse.

Mr. R. A. THORNE: When we have this kind of discourse. Yes. Thank you.

Mr. R. A. THORNE: Welcome. We are not fighting.

Mr. Steven. A. WILLIAMS: Sometimes you do not even know what it looks like.

Mr. CHAIRMAN: Senator Walters

Senator R. O. WALTERS: Mr. Williams, you were speaking quite swiftly earlier but did you also say that you were a victim of cybercrime at the beginning?

Mr. Steven. A. WILLIAMS: I was not a victim of cybercrime because it did not occur under the law. It did not fit that definition of cybercrime but in terms of someone basically tarnishing my reputation, I was a victim of that.

Senator R. O. WALTERS: So I guess the lawyers here and Mr. Thorne you can guide us here as well. In the public domain right now, people are saying that we have the Defamation Act which sufficiently deals with defaming of a person; sanctions in terms of that. Did you seek legal recourse through that Defamation Act?

Mr. Steven. A. WILLIAMS: The person did not reside in Barbados. The person was in North America. I would have to get some other thing to say that our Defamation Laws extend to USA in terms that fix that Bill for Defamation in the other States. Then, when we look at the last, the current Computer Misuse Act did not necessarily extend that far to say that one can go after what maybe a crime under **a digital** sense, in another jurisdiction so whether defamation would have occurred is the good point that may have some recourse under that. The fact is that it was a cross border issue and there were no cross border implications in the last Bill; sorry in the current Computer Misuse Act. It means that a weakened position from that perspective and at the time, the social media platforms did not necessarily see themselves as being governed by certain laws as well.

Mr. CHAIRMAN: Mr. Williams, the Bill that is presently drafted has been criticised by some as being an unreasonable limit on the Constitutional Right of Freedom of Expression and I want to say Freedom of Expression because that is what the Constitution says and not Freedom of Speech. There is no Constitutional right to Freedom of Speech in Barbados as there is, I believe in the USA and that right as defined in the Constitution is curtailed as is every provision within those sections of the Fundamental Rights Act of the Constitution. I believe, Section 12-23. What would be your response, if any, to the criticism of this Bill as presently drafted that it infringes unduly and unreasonably, the Constitutional Right to Freedom of Expression?

Mr. Steven A. WILLIAMS: Mr. Chairman, I do not think so at all. I think under this Bill; I think the intent is to do harm to an individual. Now for example, child grooming. If you look at the rights and freedoms of an individual. Is it a right that a person would go and groom a child to do something adult like? I do not think so. We have a lot of thoughts in terms of rights and freedoms but I may have the right to do something but I do not have the freedom of consequences for my actions so, no.

In terms of Malicious Communication, a person who intentionally or recklessly uses a computer system to publish, broadcast or transmit a computer data and we know what it says here, so if the intention is to hurt someone, why should I have the right and freedom to that? If I want to express myself; if I want to share my thoughts on something, that is perfectly fine but, if I am going to take up a computer or digital system to attack someone; to defame their character I give the situation of me where I have never been associated with that type of action. That hurt my character. Everyone in life just has their character so someone can take up and hide behind a

jurisdiction, to attack someone the difference is you may say people know that it is not true.

The difference is, when you publish it on the internet, if they are 10 people that know me they are 2 billion that do not and by doing so if the intention is to hurt me, why should not have recourse? A law can make some person guilty. It is the judiciary that fines if the person is guilty or not. You could bring actions against some person who you think hurt you but I still have to prove the case in court.

Mr. CHAIRMAN: Are there any other comments from Members?

Dr. R. O. SPRINGER: Mr. Williams, in your submission when you were speaking to Section 11, you suggested that perhaps this section should be treated or at least there should be some category that speaks to commercial versus domestic misuse of access to codes and passwords and so on and so forth; I think that is the suggestion that you made. If you can expand a little bit on what you meant and why you believe that it should be domestic and not exactly what you just described, where a person would have defamed you overseas that too could also be seen by some as non-commercial. It could be domestic as well.

Mr. Steven A. WILLIAMS: Okay. In relation to disclosure of codes. You have Netflix and everyone shares their Netflix password or sometimes people have a particular site that they go on; in dealing with children, they go and share a password for gaming sites.

Dr. R. O. SPRINGER: Before you go any further, Mr. Williams. I mean, remember the Bill speaks to recklessly, intentionally; it also speaks to unlawful gain. You are doing these things for unlawful gain. You are not just doing it because you have access to the information. There is the aspect of deception that speaks unlawful gain, so you cannot dismiss or divorce that particular aspect from that section of the Bill.

Mr. Steven A. WILLIAMS: Fair enough and that is why I said to me, some aspects need regulationI am reading strictly here and I am not seeing unlawful gain maybe I misread it, Sir but one stands on its own. Level one (1) stands on its own, Sir. There is another provision for two (2), so one (1) on its own speaks nothing about gain. If one (1) is linked to two (2) then fair enough but Section 11(1) stands on its own, Sir, as a specific treatment.

Section 11(2) stands on its own as a specific treatment to the offence. On its own, that is why I said, it is up to this Chamber to determine such actions but this is where regulations will come into play because I do take your point. There are certain situations where it might not even be in the corporate sense but some person now uses for unlawful gain for example, sharing passwords for commercial purposes but then that speaks to intent.

That is where I am thinking Regulations are needed for this specific Act because with regulations, it can now start to have that nuance perspective; that is why I said to the Opposition Leader that the Bill is not perfect. What will make the Bill more perfect, is if we have regulations quickly to this Act, so some of these nuances can be further identified and vetted because left on its own, it may be okay but in a sense where you just brought up, for example, it is unlawful gain, where I decide to share my password for money, I decide, you know what, I have a Netflix account, I can sell my Netflix account for $5 to three (3) friends on weekends. That is unlawful gain.

I do not have the right to do that but regulations would determine to me instead of being do granular, I do not want a granular Bill because if you have a granular minutia, a Cybercrime Bill, then we are going to be back at this again next year or another two (2) years from now when technology has changed. We do need to have a situation where regulations come extremely quick for a Bill like this, Sir.

Dr. R. O. SPRINGER: Just to summarise that, Mr. Chairman said we would have to look at this section with the view of conflating it and I think you would have suggested we reject the entire section and some of what is listed should fall under the regulation. I take your point and I just want to thank you for your response.

Mr. R. A. THORNE: Thank you, Dr. Springer. Mr. Chairman, just one (1) short question again. Mr. Williams, in answering Senator Walters, you made a very interesting comment. You cited the example of an offender overseas against whom it was difficult to find a sanction. Now you speak with the authority of a Consultant and I want to ask you if a major focus of this Bill is the pursuit of persons overseas whom you cannot otherwise capture?

Mr. Steven A. WILLIAMS: Sir, can you please repeat the question again.

Mr. R. A. THORNE: Yes. In answering Senator Walters, you cited the example of a person who may have defamed you and that person is overseas so that you cannot pursue that person in terms of defamation of character lawsuit. You referred to the usefulness of this Bill in going after that person, when you consider that it goes with the Mutual Assistance Legislation.

I want to ask you as a Consultant and you do speak with the authority of a Consultant and you will be persuasive as to the content and intent of the Bill that is before the House. I want to ask you to say to the public, if then a major focus of this legislation is the pursuit of persons overseas who are offensive against Barbadians living here? Is that a major focus of the Bill, the pursuit of a person to our overseas, who may be otherwise difficult to capture by defamation lawsuit?

Mr. Steven A. WILLIAMS: Every aspect of this Bill was looked at. I do not think there is any one (1) specific area that had more attention, honestly. I think given the fact that I would appreciate that when we had the Computer Misuse Act **there was no** social media. When we had the Computer Misuse Act there was no such thing as social media, especially in its current form. The interactions with what was people overseas versus being able to actually get there to get attention, so as you said attacking locals or whatever was not thought of.

In drafting a modern or updated Bill, we have look at every aspect of what crime will constitute for Barbadians to protect Barbadians from crime. Sir, part of that is to ensure that we had jurisdiction assistance. It is just not saying that we have a lot to go after some person but the reverse is also true. They are people in Barbados who may be involved in crime here and then from an overseas perspective, there is a judicial arm on the other end that may be able to get information on what is happening here. We cannot get one (1) without the two (2); it is not a one-way Bill.

Mr. R. A. THORNE: My question to you is whether in the drafting of this Bill, is the overseas person a major focus of attention, as oppose to a local person gossiping and that kind of thing? Is the pursuit of the overseas person a major focus? That is a yes or no. The Bill intends equal pursuit in relation to overseas as it does locals.

Mr. Steven A. WILLIAMS: Yes. It is the protection of the citizens of Barbados.

Mr. R. A. THORNE: Whether the person is overseas or here?

Mr. Steven A. WILLIAMS: Whether the person is some person overseas and not even a Barbadian, once we have a jurisdiction relationship. The person does not even have to be Barbadian or connected to Barbados. If you harm Barbadians and the person is living overseas

Mr. R. A. THORNE: Therefore, the pursuit is equal.

Mr. Steven A. Williams: Correct.

Mr. R. A. THORNE: If you have a person here committing the offence, this Bill intends to go after that person with equal intensity; equal force.

Mr. Steven A. WILLIAMS: I believe so, Sir.

Mr. R. A. THORNE: Thank you. Anybody can be charge?

Mr. Steven A. WILLIAMS: Anybody can be charged but not everyone can be convicted.

Mr. R. A. THORNE: You are back to the judiciary again. Last question, Sir. Would you agree with me that based on the content of this Bill, these offences are likely to be committed every minute, of every hour, of every day? You are a social media man and an expert; not in committing the offences but you pour over social media and you would agree with us that according to this legislation; these offences are committed almost every second of the day. Every new opening of Facebook, you will see and offence being committed. Is that not, correct?

Mr. Steven A. WILLIAMS: I would not say every second of the day. What I would say is that there is a difference between……

Mr. R. A. THORNE: Okay, let me put it differently. This could become the most frequently committed criminal offence in Barbados, if this Bill passes? For example, a story comes out in the newspaper, we see it all the time. They are reporting some incident and then the comments that comes underneath it. The insults; the offensive language; the defamation. Do you not agree that this Bill will create the most frequent criminal offences in Barbados?

Mr. Steven A. WILLIAMS: Sir, I would say that harassment is against the law of Barbados.

Mr. R. A. THORNE: Yes, I am aware of that. We are all agreeing here that this Bill will criminalise many areas of speech. We are all agreed on that. I am asking you if, as an expert

and a frequent visitor to social media, especially Facebook, would you not agree that this Bill, if it becomes the law of this country, will create the most prevalent state of criminal offences in this country?

Mr. Steven A. WILLIAMS: No. Let me say and explain.

Mr. R. A. THORNE: Okay.

Mr. Steven A. WILLIAMS: The intent is where I hang my hat.

Mr. R. A. THORNE: I am talking about content not intent. The content of this Bill will create several criminal offences across social media every minute of the day.

Mr. Steven A. WILLIAMS: How?

Mr. R. A. THORNE: By people insulting others. By a story coming out on any incident on which the press reports. You see it, Mr. Williams. People gather underneath that story and call the person all kinds of

names such as a fraud, a thief, all kinds of things. I want to suggest to you that those fall within the definition of criminality within this statute. I know you agree with that but what I am asking you is if this will not create several offences across social media every minute of the day.

Mr. Steven A. WILLIAMS: Okay. I will take a deep breath for this one.

Mr. R. A. THORNE: It is a "yes" or a "no".

Mr. Steven A. WILLIAMS: No. It is not a "yes" or a "no", Sir.

Mr. R. A. THORNE: Oh. I beg your pardon.

Mr. Steven A. WILLIAMS: It is not a "yes" or a "no" because even in life, people use - I like to quote Dame Billie - muscular words against some person which maybe against the law but it is passed because the intent, even though "man I g'ine kill man" and walk along. That in itself maybe an offence here on law. You are the constitutional man. You know whether that is an issue or not. Is it pursued by our justice system? Probably not. I go back to what I see happening with young people right now with the cyberbullying.

Part of the argument is that the same language is used in cyberbullying. There are many young people who use those words who do not have the mental separation to not take it offline. Part of the law's ability is to say now, "Let us look at the pattern of behaviour." A lot of these fights that happen in secondary schools and you can ask any school principal, is that they start online with violent language and intent and it then basically escalates. If we can use this law to stop it at the violent online behaviour before it escalates to some person getting killed, I am all for that, Sir.

Mr. R. A. THORNE: So, you are agreeing with me that the offence will committed quite often? At the end of it, would you agree with me, Mr. Williams, that this Bill; this Act or law, will create offences quite often when you consider that young people, old people and middle-aged people spend much of their time on social media commenting and saying things that are offensive every day, all day, all week, all month and all year?

Mr. Steven A. WILLIAMS: Sir,….

Mr. R. A. THORNE: The question I come to…. I know you agree with me but what I come to is the question of who selects and how is the selection done in terms of who will be charged? I think that is a concern that public will have because I know that all of us in here agree. I can open social media now and will see several insults being uttered. Who determines which one (1) to charge? That is what the public may be concerned about. Who determines? You cannot answer that. It is not intended for you to answer. It is a statement.

Mr. Steven A. WILLIAMS: I understand.

Mr. R. A. THORNE: That is what the public is concerned about. With all the offences committed across social media every minute of the day; the public is

concerned as to who will influence a prosecution. It is as serious as that.

Mr. Steven A. WILLIAMS: But, Sir, let me say that….

Mr. R. A. THORNE: It is not for you to defend, Mr. Williams.

Mr. Steven A. WILLIAMS: No, but I have to say it.

Mr. R. A. THORNE: I do not think you are going to influence any prosecution.

Mr. Steven A. WILLIAMS: No. Hold on. It is not about influencing the prosecution but do I not have a right to face my accuser? If I feel that a crime has been committed to me and I get your point because ultimately the Director of Public Prosecution (DPP) is going to have to determine if there is enough evidence warranted under this Bill, based on what has transpired online and can

enough evidence be gathered to determine if it would be actionable to carry it a court of justice. I understand you may think that it creates the opportunity for crimes to happen every minute of every day but the fact remains that just a one-off statement might not have that.

I could bring the nuisance claims and you are a lawyer. A lot of your clients bring nuisance claims wanting a defence but they do not carry over to a judge, Sir.

Mr. R. A. THORNE: Alright, we are not arguing. We are not disputing on that.

Mr. CHAIRMAN: Mr. Williams, I just want to address a few issues. In your written submission, you said that the definition of cyberterrorism should be expanded. Can you comment further on that?

Mr. Steven A. WILLIAMS: In terms of the cyberterrorism, I take the point and think I would like to withdraw that statement. I know I submitted it but I would like to withdraw it. On full reflection, I can say why. It is linked to our Anti-Terrorism Bill and my concern was by not having it defined under the umbrella of cyber, that it might not necessarily include certain types of actions. For example, we speak strictly to critical information infrastructure. At the time and my thinking; I reflected on it. Maybe it can be broad enough if you are going to refer to the Anti-Terrorism Bill.

My concern, if I still have one (1), is the fact that we do not know what shape or form terrorism is going to take under cyberterrorism. Once again, that is why I withdraw it with the hope that there are Regulations to this Act. Whereas, it may stand as adequate under Anti-Terrorism Act, I am uncomfortable to think that where we have the internet of things and have Artificial Intelligence (AI), the actions of someone where it can be artificially generated, I am not sure if it is going to cover it. If we have regulations, that can speak to it, then I will be a bit more comfortable with that.

Mr. Chairman, I withdraw that complaint with the hopes that we do have regulations that help shape some of the nuance that is outstanding in this.

Mr. CHAIRMAN: I thank you for that, Mr. Williams. I have two (2) more issues. Clause 11 of the Bill, as drafted presently, do you have it with you?

Mr. Steven A. WILLIAMS: Disclosure of Access Code?

Mr. CHAIRMAN: Right. Sub-clauses one (1) and two (2) seem to be, at least, can be interpreted in some way as repeating themselves with each other? What would be your comment on that? If you were to eliminate one (1) sub-clause, which one would you eliminate or advise to eliminate?

Mr. Steven A. WILLIAMS: Could you give me a quick second to just….

Mr. CHAIRMAN: Yes. Sure.

Mr. Steven A. WILLIAMS: I suspect there is a subtlety here, Sir but I cannot put my finger on it. What I can say, is that if either of these two (2) inserts are left in, my concern would be the judiciary's interpretation of it. Meaning, if I share a password and some person feels that in doing so, I broke the law and brought a case against me; the DPP must have a very strict interpretation of the law. Under sub-clause two (2), I could be facing seven (7) years in prison of which it does not seem to say if I am a repeat offender. I thought sub-clause two (2) was going speak to if I repeated the offence to sub-clause one (1), which is normally the case, where you strengthen the first version with the second.

This looks more like if the language may speak to if I am found guilty under sub-clause one (1) and a person who continues to do it again may find a lengthier term of imprisonment, as usually the case. With critical infrastructure, if I break into something once and get slapped with a hard fine but I do it again, then it means I am a repeat offender and the charges double.

In this particular case, I would get rid of two (2). If you have to leave one (1) back; I would get rid of two (2) but I am sure there is a nuance in here that I am not seeing it. I am not a lawyer, Sir, so forgive me if I am not seeing it with a legal eye; the fine subtleties of these two particular paragraphs.

Mr. CHAIRMAN: My last intervention with you, Mr. Williams relates to Section 19(1)(a). The issue of the intimidation aspect which appears to be criticised by some as to intimidating a person and intentionally or recklessly through use of a computer system but that it can be criminalised. I note that the Guyana section is similar but not the same and I am wondering if you would wish to recommend any amendment to that Sub-section on the issue of intimidating a person.

Mr. Steven A. WILLIAMS: Sir, I think that is politically identified because I can give a

perfect example where it should be left in. There are situations where young women are being intimidated online of not doing something. Classic example and this is an example. I am not bringing up a specific case but, if I am or my daughter is bringing a case against an individual and that person is a well-known person in society and people get to social media to intimidate her to change her mind; does it not fit this definition in its current form? If, for example, a person gets online and realises that pretty girl problems; young people get online an intimidate the person. *"You do not go in this so and so competition"* and things happen and pop off and you intimidate that person not to participate in an event or a sport; does it not fall into that definition where the person uses a computer system to intimidate the other?

I think the hullaballoo is from a political sense but I do not think we can sit down in here and draw a line in the sand over politics verses everything else. You cannot determine; you can say well this is okay unless it is in a political sense. I think that is part of the problem. If we said in a little bracket excluding politics, I do not think anyone would have a problem with this statement but unless you are going to define it because I do not think anyone would have a situation where their girl child or son or member of their family is getting intimidated via social media; the networks and think that it should be allowed. I think the problem is that politics got involved and then people see it from a political lens.

Mr. CHAIRMAN: Let me just follow up on my question. Section 19 (1) of the Guyana Act says,

"A person commits an offence if the person with intent to compel another person to do an act which the other person is not legally bound to do or to abstain from doing an Act which the other person has the legal right to do, uses the computer to publish, transmit electronic data that intimidates the other person. That person commits an offence subject to criminal law."

In other words, the Guyana section expands a bit on it by speaking towards:

"compelling another person seeking to compel a person to do an act which is not legally bound to do or to abstain from doing an act which the other person has the legal right to do."

Whereas our proposed section is general. Just a person who intentionally or recklessly uses a computer system to intimidate is guilty of an offence. I am just wondering; do you think there is reasonableness in preferring the expanded Guyana Sub-section on this issue?

Mr. Steven A. WILLIAMS: I cannot bring it down to Yes and No question, Sir. Reason being is that, for me, there are certain suggestions I would make under regulations and this is not one (1). You are asking if the intention of this particular section can be expanded and not weaken the whole entire law itself because each section builds on the other. For example, this particular malicious communication, strengthens the cyber bullying and reiterates the cyber bullying section.

I do not know if we take out some or expand upon it if it is going to weaken any part of the legislation, so I am saying, maybe it is a good argument but I am not a lawyer so for me what I would say under Malicious Communication in the intimating a person using the computer system to intimidate someone, I take your point. While they have gone and defined it, I am always in favour of **broad** law, where possible and regulations where practical, so for me that is one I do not have a straight forward question. I wish I could give you one (1), Sir.

Mr. CHAIRMAN: Okay, Senator Walters.

Senator R. A. WALTERS: Mr. Williams, as an IT Consultant feeding into the Bill; what specific technical or expertise IT policies or framework has been fed into this Bill because you hear you use it all the time that you are not a lawyer but it is not to personalise you but from a Consultant; an IT Consultant person, what are the specific areas of expertise within the IT world, that has been fed into this Bill?

Mr. Steven A. WILLIAMS: Okay, so take for example, within this particular Bill it refers to things such as how Internet Service Providers (ISPs) would be involved in terms of traffic data. What they would provide to lending assistance to the Police. I think for my perspective and where I lend assistance, is in terms of how things may be practical, so that is why I said leaning towards regulations to be helpful to this Bill would need regulations.

For me, areas of this Bill speaks to anything dealing with how technology might be impacted and how people may be impacted with technology so I did not get around to every piece of legislation but I may be asked questions in terms of how would technology impact this Bill; so is

this practical. For me, I am always for broad-based legislation because we are not coming back to this. 2005, we are not coming back to this in another 20 years.

For me, if this piece of legislation is in here, this may be how it looks like in five (5) years given where technology is going. Section by section, my responsibility was to ensure that it stood a reasonableness in terms of the time that it would be valid for or if it is a technical term, such as traffic data; how would that impact basically the legislation in terms of carrying out certain function; in terms of what has to be given with information.

If you have to hold on, for example, going back to my organisation. If I am required as an IT person to hold onto data, how long would I hold onto data for? What that should look like? These types of things that would impact a case because for me, I would really like to see some regulations because there was a case called and I give you my example again, where it was a situation with a client of mine. I had to hold onto his hard drives so how long do I have to keep the data for? What condition it might be in? There are certain questions that the Chairman would have referred to and say, *"Steven. What does this mean?" "Would this be a situation technically that we have to worry about?"* and those types of things. It is not that I have in writing of the law but being an advisor to the technical aspects of the law.

Mr. CHAIRMAN: Okay. We thank you, Mr. Williams for your input. You can be assured that both your written and oral presentations would be considered with the weight that they deserve so we thank you for coming before us this afternoon. Before we proceed Committee, I would like to invite Mr. Anthony Greene to come forward. I would like to in the interest of transparency and accountability, I need to respond and Members just crave my indulgence to some comments made, attributed in the Nation Newspaper on 25 April, 2024, to Mr. Caswell Franklyn on the legitimacy of this Committee.

Mr. Franklyn in that article is quoted as saying that, *"this Committee is reflecting on the Cybercrime Bill, contrary to the Standing Orders of this Parliament"* and he queried how Sir David Simmons should know the Standing Orders of the House and that the Standing Orders of Parliament do not allow this monstrosity. Do not allow this monstrosity, he is quoted as saying that *"they have called a Joint Select Committee"*.

The article continues to quote Mr. Franklin, who of course was a former member of the Senate, as saying that *"the Joint Select Committee is a creation of Parliament. It has never happened in the Westminster system before, where a Bill is passed from Lower House, goes to the Upper House and the Upper House then forms a Joint Select Committee. It is contrary to the rules of the House because once the House has passed it, the House cannot go back into Committee on that Bill."*

The House is not going back into Committee on the Bill but a few of its Members are sitting with Senators on the Joint Standing Committee.

"The Joint Select Standing Committee and I have the Standing Orders which establish this Committee. The Standing Orders say that the Joint Select Standing Committees are permanent oversight committees established at beginning of each new Parliament and continued to function until the dissolution of Parliament.

Standing committees are permanent committees established by the Standing Orders of the House. They are mandated by the House to oversee a Government department or departments to review particular areas of Government policy or to exercise procedural and administrative responsibilities related to Parliament.

Some Committees may have both departmental and policy area responsibilities. In addition to the permanent mandates provided to Standing Committees by the Standing Orders, other matters may be routinely referred to them by the House for examination, Bills, estimates, documents in the House, table in pursuit to statute and specific matters which the staff studied.

The House may refer specific studies to Committees by adopting a motion to that effect. The motion, once adopted, becomes an order of reference. Further to the subject matter of the study, the order of reference may also contain conditions that the Committee must comply with in carrying out the study or additional powers which it may require for that purpose."

Mr. Franklyn is alleging that the Bill having passed the Lower House and it goes to the Upper House, where the House forms a Committee. The Senate did not form this Committee. This Committee was formed under these Standing Orders by both Houses of Parliament. In fact, the Parliament of Barbados formed three (3) Joint Select Committees. This one (1) on governance

and policy matters; a second on economic and productive sectors matters and a third on social sector and the environment matters. The Lower House formed these Committees on the 02 May 2023 and the Senate formed them on 17 May, 2023.

Standing Order 48(1) empowers the Senate to commit a Bill to a Select Committee, which is a fact, which Mr. Franklyn in the article acknowledges. The Senate has so committed this Bill to this Joint Select Committee, which has been established by Parliament.

The issue of Mr. Franklyn asserting that the Bill, having been passed in the House and then if the Senate had problems with it, the Senate could identify these problems and send it back to the House or they could have formed a Committee of the Senate to investigate the Bill is not relevant here. It does not apply.

This Government, by forming these Committees is committed as expressed in the Charter of Barbados on the past in the Parliament of Barbados on the eve of our becoming a Republic; is committed to the development of active citizenship to deepen the effectiveness of our democracy. This is what this process is about. Furthermore, it is an accepted tool of parliamentary law that the House can regulate its own procedure known as exclusive cognisance. Exclusive cognisance, simply put, is the right of each House to judge lawfulness of its own proceedings and Parliament has exercised its right and the exclusive right of the two (2) Houses to make and vary their **own rules** of procedure to protect the legislative supremacy of Parliament and that is what has been done.

The Senate of Barbados on 16 February, 2024 passed two (2) Resolutions which have sent these two (2) Bills to this Joint Select Standing Committee and by doing so, it is fully within its right to do so; fully in terms of the law; fully in terms of Standing Orders and regulations and powers of the Parliament of Barbados. This is simply a way of trying to improve the functioning of Parliament, which is, ultimately the forum for the people of Barbados and allowing the people of Barbados to have a say as they choose and as they wish, either verbally; orally or both before a subcommittee; a Standing Committee of this Parliament, made up of Members of both Houses of Parliament.

I must say clearly, advice have been taken in forming these three (3) Committees and specifically this Committee, clearly by the Learned Attorney General. We have on this Committee, the Honourable Leader of the Opposition. I am Chairman of this Committee. All persons who have been called to the inner bar; longstanding lawyers and we take the advice of the Clerk of Parliament, who is a very experienced Clerk. He has been the Clerk of this of this Parliament for years.

I just felt that in the interest of transparency and accountability, I could not let what Mr. Franklyn is reported to have said go without a response because he has effectively said that this Committee has no legitimacy and I wish to publicly respond and refute that charge.

Mr. Anthony Greene, we invite you to come forward and to give your oral submission. Welcome Mr. Greene, you are here this afternoon before us and we thank you for accepting our invitation to come because you submitted in writing, that you wanted to give an oral presentation before this Joint Select Standing Committee on the Cybercrime Bill and the Mutual Assistance in Criminal Matters (Amendment) Bill.

We are allowing you no more than 10 minutes, Sir, to give your oral submission. After your oral submission, Committee Members will be invited to engage you, they might comment, questions, any clarification we need for whatever you say and you will be invited to so respond to Committee Members.

Mr. Anthony GREENE: Thank you very much, Mr. Chairman. Good Afternoon to the Members of the Committee. I am thankful for the invitation and the opportunity to present. I must say though that the timelines were very tight and that is why I opted for the oral presentation just to state that I have not necessarily come to address matters specifically relating to the content of the Bill, especially given the limitations and preparation for the presentation. Just to make a presentation in relation to the general spirit of the Bill and the perceptions that have arisen out of the debate of the Bill.

I want to begin by saying that communication lies at the heart of everything that we do. It serves as the conduit through which ideas are shared, decisions are made and progress is achieved. As such, it is imperative that we carefully evaluate our national approach to information sharing, ensuring that the environment we cultivate fosters transparency, inclusivity, collective goal setting and

participation. With the introduction of the Barbados Cybercrime Bill, we are presented with an opportune moment to reflect on the manner in which we communicate in our country.

Our communication strategy should not only facilitate the dissemination of information but also empower individuals to actively engage in shaping the

future of our country. I know that I only have 10 minutes, so I have a lot to say on that but I am going to skip to the meat of the matter. First, I just want to say that as we implement the Cybercrime Bill, I think it is important that we be careful to avoid stifling freedom of the press and expression or I should say the perception thereof.

There is a need to strike a delicate balance between protecting individuals from cyber threats and upholding the principles of transparency and accountability in governance. We must guard against the perception that the Cybercrime Bill is aimed at restricting the flow of information or fostering a culture of secrecy and instead, approach its implementation with a nuance understanding of the complex interplay between security concerns and democratic principles. I do agree that with the advancement of technology, we really need to ensure that our laws and legislations are up to task in terms of dealing with what we currently face.

Back in 2017, the Centre for Law and Democracy (CLD), posted on their website concerns about the Cybercrime Bill in Trinidad and Tobago. The article stated that when it was first introduced, the Cybercrime Bill was heavily criticised by the media and human rights organisations, including CLD, for vague and over-broad content offences which would have prohibited a range of innocuous, normal or even beneficial online activity. Despite some minor revisions, the current version of the Cybercrime Bill still suffers from these problems, according to them.

Michael Karanicolas, the Senior Legal Officer of CLD, is quoted as saying that, *"over-broad content offences are always illegitimate but are particularly dangerous online and where many people are still in the process of discovering their voice. The Bill, if passed in current form, could have a substantial chilling effect on online speech in Trinidad and Tobago."* The article also states that some minor improvements have been made in the latest draft; the Bill in Trinidad and Tobago is what we are talking. Notably, the deletion of Section seven (7) which prohibited the illegal interception of information.

Now, interestingly, we also have a similar reference in our Bill; the Illegal interception of data in Section Eight (8). We note that that Section seven (7) in the Cybercrime Bill in Trinidad and Tobago was deleted. Again, I refer to the article which draws out concerns in other sections and says that in each case, the prohibitions are so broad that they include perfectly legitimate online activity. Furthermore, the Cybercrime Bill creates a presumption of criminality for expressive activities which are undertaken without lawful excuse or justification, shifting the onus on users to demonstrate that their actions are legitimate.

This type of reverse onus runs contrary to the international freedom of expression standards which only allow States to prohibit limited and clearly defined conduct. This problem is compounded by the fact that the term "justifications" are unduly vague. Very quickly, Sections eight (8) and 12 are particularly problematical, in so far, as they essentially make it illegal for journalists to receive leaked information, including from whistleblowers. Leaks often serve as an information safety valve, performing vital public functions, for example, by drawing consumer attention to a defect in a product.

Even when it is reasonable to sanction those who breach a computer system to obtain information or share information beyond its authorised recipients; journalists should be allowed to receive and report on the information they receive without fear of retaliation. I will add, so long as the journalists or the media personnel are acting in the public's interest. This is definitely core to the work of the media. It is not just in Barbados that concerns have been raised about matters relating to such a Bill but there are legitimate bodies, individuals and professions that have reason to flag real potential conflicts, as a part of the national discussion on this Bill.

I want to quickly move to the fact that the Media Institute. Let me just state my recommendation because this is one of the main reasons I chose to make a presentation. There is one (1) thing that I think would help us to address the concerns and perceptions against the Cybercrime Bill. I now make this recommendation with a view of gathering greater support and vying for the Cybercrime Bill. It

appears to me that there is support generally for many of the issues raised in the Cybercrime Bill. The concerns center mainly on freedom of expression. Truly, we are missing a very important piece of legislation that addresses many of the concerns raised around this Cybercrime Bill.

That important piece of legislation is the Freedom of Information Act or Access to Information Act. The responsibility is being placed on individuals in relation to how they communicate online and in some instances, rightly so. Government ought to shoulder some of this responsibility for how we communicate, by creating an environment where access to information that is in the public's interest is fluent, timely and unhindered.

The Media Institute of the Caribbean (MIC), just last week released a Freedom of Information (FOI) and Access to Information (ATI) Legislative Review Report. It specifically looked at the English-speaking Caribbean. In the presentation of this report, it noted that not every country in the English-speaking Caribbean has Freedom of Information or Access to Information legislation.

The countries with the laws in place are Trinidad and Tobago - Freedom of Information Act, 1999.

Belize - Freedom of Information Act (revised edition), 2000.

Jamaica - Access to Information Act, 2002.

St. Vincent and the Grenadines - Freedom of Information Act, 2003. It has been passed but no in effect.

Antigua and Barbuda - Freedom of Information Act 2004.

Guyana - Access to Information Act, 2011. They are issues with that one (1).

Bahamas - Freedom of Information Act, 2017.

Cayman Islands - Freedom of Information, 2021. That was a revision.

St. Kitts and Nevis - Freedom of Information Act, 2018. Amended in 2023.

That is the list. There is no Barbados on this list. Barbados is at the back of the pack as it relates to Freedom of Information, Access to Information Legislation and we need to come to the front. Where are we? Barbados has drafted a Freedom of Information Act but has never enacted it. The same issues St. Lucia and Grenada. Under the Section, General Comments of this MIC Report, there is a special note of the regional agreement on Access to Information, public participation and Justice in Environmental Matters in Latin America and the Caribbean; The **Escazu** Agreement and this regional treaty creates benchmarks for FOI and **ATI** Legislation; interestingly enough it addresses environmental matters of which Barbados as we know, is up front and centre and rightly so. We are doing a good job in addressing those matters.

This same legislation, addresses benchmarks for FOI and **ATI**. Some states in the region has signed the agreement while some have both signed and ratified the agreement thus creating obligations for themselves. Let **us** look at that list, those who have signed. Antigua and Barbuda; Belize; Dominica; Grenada; Guyana; Jamaica; St. Vincent and the Grenadines; St. Kitts and Nevis; St. Lucia. There is no Barbados.

States that have ratified Antigua; Belize; Guyana; St. Vincent and the Grenadines; St. Kitts and Nevis and St. Lucia. To its credit, the **Barbados Association of Journalists and Media Workers** (BARJAM), has continuously for FOI and ATI Legislation through BARJAM. We did hear from the Attorney General in 2019 on this matter. A release from the **Government Information Service** (GIS), in 2019, stated that the Attorney General and Minister of Legal Affairs, **the Honourable Dale Marshall,** made a commitment that the matter would engage Government's attention and a time line of 1 year was given and he also said that government had already started to examine what a Freedom of Information Bill for Barbados would look like and that was August 2019.

It is important to also say though that COVID-19 came and before that familiar caveat is highlighted to put things into perspective, let me say then came COVID-19 but my point is that we now need to press on, to return to normal; to bring these important matters to the forefront and a government that wants to bring a cohesiveness around the issues of how people use devices and share information, within the contents of the advancement of technology, could gather greater support for the Cybercrime Bill by following up on the Freedom of Information Act.

It projects a willingness to not just hear the people but to listen and act and to lead by example in creating an enabling environment for responsible sharing of information. Back to the GIS release, the Attorney General said back in

2019, concerning the FOI and ATI Legislation that the process would first require government, having to completely transform the way things were done in the Public Service, particularly how information was documented and other governmental processes and I would like to think by now that COVID-19 has sped that up and I do think that government has shown good intent, if you are honest and has made some progress in this regard.

The Attorney General was quoted as saying back then, *"A serious administration needed to have a healthy relationship with the press. What we have to do as an administration is to ensure that we facilitate the dissemination of information to our citizens. When we look at the question of a Freedom of Information Act it is precisely because we need accurate information to be in the public domain. Secondly, in order to ensure transparency and good governance citizens have to have almost untethered access to information and thirdly, when people in leadership roles understand that there is a mechanism where their actions are exposed and measured in fairly short order, then they have a strong incentive for conducting themselves properly."* Mr. Marshall declared, noting such matters would exclude those of National Security. To facilitate the process.

Mr. CHAIRMAN: Mr. Greene, just need to advise you that you have one (1) more minute.

Mr. Anthony GREENE: Okay, alright so to wrap up…

Senator G. P. B. NICHOLLS: Chairman, may I ask Mr. Greene to share his written presentation with us, if he is so minded.

Mr. Anthony GREENE: Sure. Definitely. So to wrap up, let me say this: In modern times we need to modernise our laws yes and our people are expected to accept this and conduct themselves accordingly; that is why we are debating the Cybercrime Bill. Likewise, we need to modernise the processes within government that will facilitate how information in the public interest is captured and disseminated. Both go hand in hand to strengthening the values of responsibility, trust and transparency while truly turning our backs on perception of secrecy, corruption and unnecessary control of information. You notice I said perception.

Especially in the digital age, my final point is that this a way for us to work together, to fight against the enemy. The enemy of misinformation and disinformation. The media in particular applied skills of verification and other treatment of information as part of its work and it is now doing so with the same concerns that we all have about the technology.

In conclusion, the enactment of the Barbados Cybercrime Bill presents the opportunity for us to reaffirm our commitment to effective communication practices. Let us seize the moment to cultivate a culture of openness, dialogue and progress thereby empowering our people to play an active role in shaping our collective future. In so doing, my recommendation to treat the Freedom of Information, Access to Information Legislation with the same level of seriousness, will help us to achieve this. Thank you for the opportunity to present.

Mr. CHAIRMAN: Thank you, Mr. Greene. You realise I gave you some liberty because you spoke mainly on the need for a Freedom of Information Legislation in Barbados and that is not our mandate. Our mandate is not to advise on what other pieces of legislations should come before Parliament; we are looking at two (2) Bills and neither of them are Freedom of Information Legislation but I allowed you a bit of width and length in cricketing terms. We have cricketers here in this Committee but I would want to urge you, to make your further appeal for that legislation before other forums or by other means. Before I intervene and engage you, I will allow other Members who may wish to do so. Any Members? Senator Nicholls.

Senator G. P. B. NICHOLLS: Thank you, Mr. Chairman. Just a couple questions for Mr. Greene. Good to see you again and god luck tomorrow. You mentioned Trinidad and I did not catch the name of the person who wrote the article about the comments about their consideration of the Legislation but I am wondering if you are aware of any challenges to the Bill even at this stage in Trinidad Parliament? Any legal challenges?

Mr. Anthony GREENE: Right so as I said, this was an article that was posted back in 2017 by the Centre for Law and Democracy and they emphasized issues with that particular Bill at the time. Now, my main point there is, obviously if there are issues that they have with the Bill, then at the end of the day we also have issues. I was not delving into the specifics of it.

Senator G. P. B. NICHOLLS: I was not suggesting that you were. I was just trying to understand the point you are making from how I

understand and I am aware, I am not sure if you are but Trinidad is the only country within the Commonwealth Caribbean that does not have specific limitations on fundamental rights written into the text of the Constitution. In other words, the rights can appear as if they were absolute. There is no written limitation in the text of the Constitution, whereas in Barbados, we will have constitutional right of freedom of expression, Subsection one (1) and then limitations in Subsection two (2). They are not written in a way in which there is any expressed limitation, so that in Trinidad and Tobago, the way in which the constitutional rights are interpreted by the Courts, is on the broader spectrum of what is reasonably justified of what is a free and democratic society.

Whereas, the exception in the other parts of the Commonwealth Caribbean would require the challenger to the Bill or the legislation to when it is passed to come within or to show that the Bill goes outside the exceptions. Then, that broad question comes into play, so that I was just curious as to the criticisms of the Bill you said **Circa** 2017 and whether or not there have been any challenges to the legislation since then, based on the criticism because we need to necessarily separate, in my view, the criticism that a Bill might be Constitutional as a comment, a legitimate concern by people as opposed to a ruling in the same way.

Mr. Anthony Greene: I take the point and I note with interest that in that same article, like I said, they would have deleted an entire section related to the illegal interception of information. I do not know if that is related to what you just said but we do have that particular section like I said in ours. To the same extent that these pieces of legislation exist elsewhere and would have been reviewed and relooked is the same extent to which people who are raising concern might have legitimate points to make.

Senator G. P. B. NICHOLLS: I am not sure but you were not online when Mar. Harper gave his presentation.

Mr. Anthony GREENE: No.

Senator G. P. B. NICHOLLS: He would have showed us some newspaper headlines from various countries around the world. Are you aware of the constitutionality of this Bill in its present form? The model Bill on the **Bucharest** Convention is in Jamaica and Guyana. We are not new here; having been successfully challenged for it being unconstitutional or more specifically, being in breach of one's freedom of expression.

Mr. Anthony GREENE: Very broadly, but like I said……

Senator G. P. B. NICHOLLS: Are you aware?

Mr. Anthony GREENE: Yes, generally.

Senator G. P. B. NICHOLLS: Are you aware of the Courts striking down the legislation? Are you aware of any legal challenges formally brought before any Courts in the region, say for example, Trinidad?

Mr. Anthony GREENE: No, I am not.

Senator G. P. B. NICHOLLS: That is it for now, Mr. Chairman.

Mr. CHAIRMAN: Thank you, Senator Nicholls. One of my two (2) points, interventions with you Mr. Greene to expand at this time on what Senator Nicholls has said, yes, we have been hearing a lot on the potential of this Bill as presently drafted to infringe on the rights of freedom of speech and I corrected at the beginning, it is not a constitutional right to freedom of speech as in the United States of America; where people could call anyone in public office corrupt and say they are crooks; they are thieves and that is their constitutional right, is the freedom of expression.

There has to be a difference in that regard and that freedom of expression in terms of our Constitution Section 20, as Senator Nicholls has said, it is a freedom *of expression to say whatever you want say about anybody, "they are a 50-cent prostitute; they thief the Treasury money"* and you do not have the proof, you cannot prove it. It is curtailed like every other provision in the fundamental right section by the interests of defence; our public safety public or the public morality; public health and not to infringe people's privacy rights and the rights to defame people. I just wanted to clarify that with you in terms of the Constitution.

Mr. Anthony GREENE: Sir, I hope that my presentation did not suggest such because I did not make any comment as it relates to encouraging that kind of freedom of expression, especially as it relates to defamation. I think, we in the media know all too well the interest around matters related to defamation and we deal with it quite regularly.

There are times when information is within the public's interest and that the key or the crucks of the matter in terms of the presentation; that

information that is relating to the public's interest, that there is a right for the public to know, a right to information, which is also supported as we know in the UN Regulations Article 19 supports the right to information and for people to know.

It is in that regard, in that spirit that the presentation is being made and I think that we have a situation where the Cybercrime Bill brings that debate front and center. People are concerned that matters that they want to debate and discuss online, the Bill may seem to clamp down. What I am strongly suggesting that we need to have the Bill and I think for the most part, the Bill seeks to ensure that in this present age that we are in, that people conduct themselves online in a way that we can progress as a society.

As it relates to being able to freely speak and defame people, that is the part there that I think we need to look at. Essentially at the end of the day, I think and I still am happy to present and Mr. Chairman, I understand that the Committee is not going to look at the Freedom of Information Act but I wanted to use the opportunity to strongly suggest that that piece of legislation will address the entire spirit of the Cybercrime Bill and what we are trying to achieve.

Mr. CHAIRMAN: Okay. My second engagement with you, would be where you expressed concern that some provisions of the Bill could curtail the media from expressing itself and giving information, *etcetera*. How I read it, is that some of the provisions of this Bill relating to Illegal Access; Section four (4), Interfering with computer system; Section seven (7); Illegal interception of data; Section eight (8), Access with intent to commit further offence; Section 10 and Disclosure of access code; Section 11.

In all of those cases, an expansion now of similar provisions under the Computer Misuse Act which of course has been enforced since 2005, 19 years ago and obviously the proposed provisions of this Bill, as presently drafted, increased the penalties in every case of those five (5) sections I have cited. In the almost two (2) decades of the Computer Misuse Act, have your concerns about the restrictions and limitations that these similar provisions in the Computer Misuse Bill, as presented drafted, would carry out on media houses such as yours, would you say that they are justified?

Have we seen court cases or case law in Barbados which has been brought against the media under the Computer Misuse Act that justify the fear that you expressed within your oral presentation?

Mr. Anthony GREENE: No. I cannot say that that is the case. What I am raising is our general issues that the fraternity of media and journalists have cautioned in relation to these types of matters. I cannot say that that is the case. You know sometimes these things are tested. I think because of that, we still need to have it as a part of the conversation and concern.

Mr. CHAIRMAN: Any other Members?

SENATOR G. P. B. NICHOLLS: Yes, Mr. Chairman. Just let me come back at Mr. Greene. Mr. Greene, you would agree that it is the role of Parliament to pass the laws which provides for the criminalisation of criminal activity?

Mr. Anthony GREENE: I do not know that I necessarily want to.

SENATOR G. P. B. NICHOLLS: No. I am building something here, so I just wanted you to. I will adopt the format of Mr. Thorne, my senior.

Mr. Anthony GREENE: Within the…. Criminalising….

SENATOR G. P. B. NICHOLLS: You agree with that?

Mr. Anthony GREENE: That it is the….

SENATOR G. P. B. NICHOLLS: It is not a trick question. Mr. Greene, we have known each other for a long time. I am not trying to….

Mr. Anthony GREENE: I think we have to tread carefully when it comes to criminalising.

SENATOR G. P. B. NICHOLLS: Right. Parliaments will make that judgment.

Mr. Anthony GREENE: Yes.

SENATOR G. P. B. NICHOLLS: It is the role of courts to determine whether Parliament has gotten the judgment correct?

Mr. Anthony GREENE: Yes, but as it relates to….

SENATOR G. P. B. NICHOLLS: Do you agree with that?

Mr. Anthony GREENE: That what?

SENATOR G. P. B. NICHOLLS: That it is the role of the courts to determine whether Parliament has got that judgment correct, in terms of balancing the rights and interests of people in the society?

Mr. Anthony GREENE: Yes, but I do not know if even agree with….

SENATOR G. P. B. NICHOLLS: You do not agree that it is the role of the courts to determine?

Mr. Anthony GREENE: No. Hold on. Let me finish my point.

SENATOR G. P. B. NICHOLLS: Mr. Greene, I will allow you to finish but let us have this conversation first because give me a chance to see where I am going.

Mr. Anthony GREENE: Right.

SENATOR G. P. B. NICHOLLS: Parliament passes the law….

Mr. Anthony GREENE: Well, I would like to see where you are going.

SENATOR G. P. B. NICHOLLS: Right.

Mr. Anthony GREENE: Because your line of questioning is interesting and I do not want to get trapped. I want to hear your line of thought before I respond.

SENATOR G. P. B. NICHOLLS: Mr. Greene, we go back too long for me to try to trick you. I am not going to try to trick you. If we were on a cricket field, then yes. I did not have to trick you then.

Mr. Anthony GREENE: You mentioned what on the cricket field? Do not let us talk about that cover drive that, you know...

SENATOR G. P. B. NICHOLLS: I was trying to create the gap between bat and pad. Do not worry about that. Parliament makes a law. Right? Whether it is a good or bad law, it makes a law in its judgment. It goes through a process and there is a debate. The law is passed. Citizens may feel aggrieved by the law and they may bring an action. It is the role of the court to determine whether or not in the balancing of the rights of citizens, under the Constitution and the freedoms that people enjoy, whether that balance has been struck in the right place.

Do you agree with me?

Mr. Anthony GREENE: Agreed.

SENATOR G. P. B. NICHOLLS: It is also the role of the citizens of the country to agitate and keep the discussion going as to whether or not both Parliament and the courts have gotten their respective roles correct. In other words, the court might determine that there is not a breach of a constitutional right but that does not end the discussion. Do you agree with me? All of this is a necessary process within the context of a democratic society that we live in. Right? The media plays a very important role in keeping that discussion going on.

Mr. Anthony GREENE: Correct.

SENATOR G. P. B. NICHOLLS: This is where I am just generally going. Some people may get the view that the law comes, it has to be perfect at the first time, it will always be perfect and it will never require adjustments because we can take it and put it on shelf up on a shiny hill. If it does not meet that level of perfection, then it is a problem to be a law.

Mr. Anthony GREENE: I still think in response to that, that in this process and I suppose this is what we are doing, there is room for hearing the concerns of individuals.

Senator G. P. B. NICHOLLS: Definitely.

Mr. Anthony GREENE: Before we put the law into **place**, we go back and review if those concerns are legitimate, and we make adjustments where necessary, before it is tested; especially when it comes to people having the ability to express themselves.

Senator G. P. B. NICHOLLS: I can safely tell you I do not think within the foreseeable future, that we should ever fear in this society that expression could be curtailed by this Government, the next or anyone under the present arrangements that we have with a Constitution in place. I always say to others that with the present conversation of the CCJ, which has really basically said that there are certain basic, fundamental anchors that not even Parliament can change.

We have had only recently for the first time in history of our democracy, where the Constitution has been amended and the courts for the first time in Barbados has struck it down as unconstitutional; even although it was passed with the two-thirds majority. Even, Mr. Thorne voted for it at that time. There is a deep basic structure of the constitutional fabric of the society and no matter what law is passed by Parliament, the guarding of those rights is always the courts.

I wanted to just separate between the agitation for where that balance should be, whether the balance should be in favour of being able to say and operate in cyberspace and do everything that you want to be able to do without oversight, without regulation and without tilting the scales in a way that there is any regulation of that activity. Right. I am not suggesting that that is a free-for-all but appreciate what when we do that, we will have a situation then where the persons who do not have genuine interests, legitimate interests and lawful interests might also

operate within that space and cause hurt and destruction.

The balance has to be drawn because we have the freedom but the laws are there to ensure public health, public safety, public morality and that public interests are protected. Parliament passes the law. The courts decide whether Parliament has gotten that balance correct; free speech critical to a democracy. It is the basis on which we exercise but that is not going to go away by just the passing of a law. Do you agree with me? It cannot be threatening….

Mr. Anthony GREENE: I think you are going to have my support there but you what will be stronger than even that? Like I said, we are placing the onus on people to get it right. Maybe we should, as it relates to the advancement of technology. My main point is, I think it was in 2008, that you had the draft legislation of the Freedom of Information Act. I mean this is what, over 15 years that the draft has just sat there. It has to be that that burden of creating an environment for how we communicate and that is how I opened.

I opened by saying just that. Communication lies at the heart of everything we do as a people and if you are really serious about what you just said and I agree, then the government will also take some of that responsibility as well. It is about the environment, the perception. That is what it is about so I may agree with you; some people may agree with you; others would not. Some people may feel that their environment is threatened right now in relation of Freedom of Speech and expression. My point is really about the access to information and the freedom of information.

Senator G. P. B. NICHOLLS: Anthony, because of our various professions, just to draw a recent example. Last year, I represented a lady who spoke on a political platform who was in danger of being disciplined and that regulation has been in place for 56 years. Nobody has ever sought to challenge it and how many public officers would have suffered from being in fear of losing their jobs for even going a political meeting and we must not feel that the agitation and the agitation does not only have to come by way of bringing a case in court but it must be a constant vigilance in the society and not only when the government acts there is a reaction but we also have to preserve these rights and talk about them and exchange.

I welcome the discussion on the Freedom of Information Act and perhaps now is the time to have that other discussion as to how Freedom of Expression can be enhanced, by way of the Freedom of Information Act because Freedom of expression includes and I do not necessarily agree with the Chairman, free speech; freedom to communicate ideas; freedom to receive information as well. All of that is part of Freedom of Expression as defined in Section 20 of the Constitution so that this process is good. It is necessary but I just wanted to know where you were in terms of the spectrum as to whether or not, every time legislation comes up to protect a legitimate gain because at the end of the day, if this were tested, portionality is the basis on which the court would determine if this is constitutional or not.

Is this the only means to achieve these objectives? Are there legitimate objectives that the Parliament has in mind by passing this legislation? Are the means designed to meet those objectives and has the balance been struck right? That is basically the test of **portionality.** What is reasonably justifiable and free and democratic society because we know they are constraints but they cannot be too far on the other side now to restrict freedom.

Mr. R. A. THORNE: Just a very short intervention.

Mr. CHAIRMAN: Honourable Opposition Leader.

Mr. R. A. THORNE: I am not going to quarrel with you, Mr. Greene. I am not intending to quarrel with you at all. Do I understand you to be articulating reservations about the Cybercrime Bill?

Mr. Anthony GREENE: My reservation…

Asides.

Mr. Anthony GREENE: In all fairness, I really did not come as I said in the beginning, prepared to speak about the content of the actual Cybercrime Bill because of the limited time.

Mr. R. A. THORNE: Right but do you have reservations about it?

Mr. Anthony GREENE: Yes.

Mr. R. A. THORNE: Let us go to the second question then. You have reservations about it. You speak on behalf of your media house. That is STARCOM is it?

Mr. Anthony GREENE: Yes, STARCOM Network.

Mr. R. A. THORNE: Right. Do you speak on behalf of the entire media or just..

Mr. Anthony GREENE: As a media practitioner, I am sure they would be concerns that they would have.

Mr. R. A. THORNE: Right because you have spoken to other heads of the other media houses. You do not mind saying that?

Mr. Anthony GREENE: Where are you going?

Mr. R. A. THORNE: To the next question but after you answer this. This is a free environment. Do not be afraid of Senator Nicholls.

Asides.

Mr. Anthony GREENE: We have had some discussion generally.

Mr. R. A. THORNE: You confessed that. Right. You have spoken to the other heads of the media.

Mr. Anthony GREENE: I have not spoken to the other heads specifically but there is general conversation.

Mr. R. A. THORNE: Do not worry about the conversation. You have had general discussion with other heads of other media houses about this Cybercrime Legislation?

Mr. Anthony GREENE: No, not if you put it that pointedly. No.

Mr. R. A. THORNE: You have not discussed this with them at all. No other heads?

Mr. Anthony GREENE: No other heads of any media houses.

Mr. R. A. THORNE: Well other people in the other media houses?

Mr. Anthony GREENE: Yes. Yes.

Mr. R. A. THORNE: These are very simple questions, yes?

Mr. Anthony GREENE: Yes, but there are very pointed questions too.

Mr. R. A. THORNE: Well simple questions tend to be pointed and they have similar reservations that you have expressed here today?

Mr. Anthony GREENE: I cannot tell you that we have gotten together and agreed that we have these particular reservations that we are bringing to the table.

Mr. R. A. THORNE: Not the particular reservations. What I am asking you. You have had discussions with other personnel from other media houses and all I am asking you is if there is general discontent or general reservation about the contents?

Mr. Anthony GREENE: I think the media has been more focused more than anything else on facilitating the national discourse so I cannot tell you that we as media houses is necessarily bringing any particular reservation about the Cybercrime Bill. We have been more interested in making sure that we facilitate the discussion and impartially so.

Mr. R. A. THORNE: Okay, I see. So that when you say that you have reservations, it is Mr. Anthony Greene as Head of STARCOM Network that holds these reservations against the Cybercrime Bill.

Mr. Anthony GREENE: When I say reservations because we are not going into the detail here. No, it is alright. I am not afraid of it.

Mr. R. A. THORNE: What it means is that you do not agree with everything that is in the Cybercrime Bill.

Mr. Anthony GREENE: That is right.

Mr. R. A. THORNE: Precisely. You do not agree with everything in it. In other words, you would like to see some changes.

Mr. Anthony GREENE: Yes.

Mr. R. A. THORNE: That is reasonable. That is all, Sir.

Mr. CHAIRMAN: Any other Members wish to engage, Mr. Greene? Okay, if not, Mr. Greene we thank you for coming and having a lively discussion. I get the impression you did not expect to be engaged so thoroughly but that is what we are about. Like I said, I urge you to take your advocacy for Freedom of Information Legislation where it belongs; you and your fellow media practitioners surely know how to lobby for what you want on that issue, okay?

Mr. Anthony GREENE: Thank you very much and again I appreciate it.

Mr. CHAIRMAN: If you could just, Mr. Clerk, to remind Mr. Greene and Mr. Williams to send what they read. Reverend Nicholls, you are here pursuant to the invitation by this Committee for persons to come and give oral submissions before it. You have accepted that invitation, so I thank you for so doing. I just want to clear up because I want the record to be clear, Sir. You wrote in your representation to be given an oral presentation; a hearing that you are His Excellency. Like I said, I would first like for you

for the sake of the record, tell us how you are now His Excellency.

Rev. Dr. Ferdinand NICHOLLS: It would be my pleasure, Sir. Let me just say good afternoon to the Members of the Committee and to thank you for the opportunity to make this oral presentation to you this evening. The explanation is not within my 10 minutes, Sir because I have not got it in my speech.

Mr. CHAIRMAN: That is not within your 10 minutes. You are setting the record straight in terms of your nomenclature. It is not engaging your 10 minutes.

Rev. Dr. Ferdinand NICHOLLS: In 2018, I was appointed the International Governor of the Academy of Universal Global Peace, United States of America (USA), as the United Nations (UN) affiliate to Barbados and the designation I carry in that context is His Excellency, and it is within that context that I operate. That is 30 seconds right?

Mr. CHAIRMAN: Okay, Sir because you and I go far back. Your aunt was my godmother, so I was wondering about His Excellency, which I know nothing about. Sir, you have 10 minutes maximum to make whatever case you want to make, for; against; mutual for either of these two (2) Bills and then afterwards, Honorable Members of this Committee will be given the opportunity to engage you on anything you have said.

Rev. Dr. Ferdinand NICHOLLS: Thank you, Mr. Chairman. Let me begin by saying, I am seated here not as a lawyer or cybercrime expert by any stretch of the imagination but, I do have concerns that I will attempt to address in a broad way this evening but a little different, I believe from what you would have expected because I think there is some that would anticipate that would present certain specifics.

As one of my colleagues say to me, I want to the large degree, stay in my lane and as such, I want to take the opportunity to commend the Government first of all, for seeking to protect the interests and wellbeing of the citizens of Barbados through this Cybercrime Bill. Given the recent spate of online incursions into both the private sector and the public sector, it is noteworthy that efforts are being made to protect the country from invasive forms of cybercrime.

I am here today, as an ambassador for what is considered by many to be the highest form of government known to mankind and that has gifted this administration with the opportunity to govern the affairs of the people of this country. As such, I fulfill a role that I view beyond that of either Parliament or Senate and for that matter, beyond this Joint Select Committee.

A previous presenter was afforded as much as over two (2) and half hours but as you have just heard the Chairman, he has allocated 10 minutes to me. There are a number of messages since this Cybercrime Bill has made public engagement, I have received regarding concerns and fears of millions of people pertaining to this Bill. It is seen by some as the threat to their fundamental freedoms and liberties and the fear of simply freedom of speech and expression being targeted for criminalisation.

It is seen by some as an invasion of their liberties and freedoms and privacy and yet others, such as spiritual ministers, seek some sections of this Bill as a threat to their free declaration of the gospel in the country where religious freedom is hailed.

Our National Anthem encapsulate the point that the Lord has been the people's guide for past 300 years and it goes on to tell us that he is on the people's side and as easily as he has granted this administration, the opportunity to care for the affairs of the people of Barbados, he can and he will if forced to revoke that privilege and he does not need an election to do so. He will hold every one of you in this Committee, accountable for the decisions that you make that are capable of affecting the lives of people, whether negatively or positively. You should take this committee meeting as a reprieve from him to get this Bill right. The voice of the people, we are often told, is the voice of God and people are speaking.

By the same token, I wish to remind everyone that freedom is not the right to do what you want but it is the power to do what you ought. This administration has been elected and by extension, employed by the people of Barbados to look after the interests of the people locally, regionally and internationally. It is necessary for the public to be engaged before decisions that can have a lifetime of ramifications on the people, be made by any administration. Regrettably, this appears to not have been done in this instance and so we are here today.

Permit to quote from a speech made by the then Leader of the Opposition, now Prime Minister, in the lead up to the 2018 general election:

"Today is about sending a message that the people of Barbados will not allow anybody, neither Labour Party; Barbados Labour Party; Democratic Labour Party; private sector to intimidate it, not ever again.

You have been raised to think for yourself and you have the right to speak out and you have the right to speak out without somebody trying to unfair you in this country. So today is equally about reclaiming for Barbadians, the right to express themselves in an environment, where fear is removed.

We do not believe that the charging of a Reverend for saying this is the worst government or threatening businessmen with contracts or threatening people with jobs; this cannot continue in Barbados of the 21st century and if ever the time comes that you give us the confidence to lead you; we too must ensure that we never rule a government to unfair or cause fear in this country. This is the solemn promise of the Barbados Labour Party (BLP)."

A solemn promise can almost be equated to a spiritual statement. It is as serious a statement as you can possibly make, such as when you stood taking your vows at the altar when you got married. A solemn promise was made and this administration was elected based on that solemn promise. There is an applicable biblical verse that cautions, even warns us, not to make vows that we do not intend to keep. For God considers such persons to be fools.

I am sure that no one seated in this Honorable Chamber wishes to have highest power we know of consider us to be fools. I can inundate you with a myriad of international documents speaking to the need to proceed with discretion and care as it relates to the implementation of the Cybercrime legislation as guided, for example, by the Budapest Convention or extracts from the United Nations Charter on Human Rights that speak to the protection of the right to freedom of expression, which, for the sake of some person, includes freedom of speech.

Our references to the matters of proportionality is expressed under the European Convention of Human Rights; the International Covenant on Civil and Political Rights and other applicable international human rights instruments. There are more questions than there are answers. Where are the safeguards and conditions also included in the Cybercrime Convention in the Cyber Crime Bill before us now, in Barbados? Why are sections of the Bill seeking to criminalise the Barbadian public rather than ensure the safeguards and conditions identified by the Cybercrime Convention?

There is much more that can say regarding this Bill but the allotted time, Sir, does not permit me to do so. I am confident, especially having listened to the speaker that preceded me, that other presenters will address those areas of concerns specifically.

Before I conclude, let me be clear. Citizens are not against this Bill in its totality but only against certain sections such as found between Clauses 19 through 23 which either needs to be dramatically amended or removed in totality.

I dare say, that there may be those who might have felt that I should have engaged more on the specific

areas of the Bill but my duty as given to me today, is to caution you as you make your decisions and to the conclusions of these contributions written or oral. The people are watching you and they are not afraid.

A higher authority is also watching you and he will hold you accountable for any action taken to the detriment of the people you represent. Again, thank you for this opportunity.

I pray God's blessing and direction as you deliberate on the contributions that have been made. Whatever you do, know that the time for any theatrics in Barbados is over. This is the Barbados of the 21st Century.

Thank you.

Mr. CHAIRMAN: I thank you, Reverend Nicholls and for you imparting God's guidance on the deliberations of this Committee and indeed on the deliberations of the Government as a whole. I invite Members to engage in discussion with Reverend Nicholls, if so minded.

Dr. R. O. SPRINGER: I will just ask one (1) question. In your presentation, Reverend Nicholls, you asked a question. I know you said you would not go into any specifics but you did ask a question, why are sections of the Bill seeking to criminalise sections of the Barbadian public?

I think that is a statement or a question that requires greater explanation. Yes, you identified Sections 19 through 23 but you really need to speak to why you believe that this Bill is seeking to criminalise sections of the Barbadian public. I do not necessarily support that view. You would really want to speak to who is that section of the

Barbadian public that you are referring to, if you do not mind.

Rev. Dr. Ferdinand NICHOLLS: Thank you. In the ten minutes I was allocated, as I said, there is a lot more that I could say because I actually brought two (2) submissions with me this afternoon. I smiled a bit earlier when I heard that a Pentecostal Minister was being given 10 minutes to speak. That in itself is a miraculous accomplishment and achievement. Nevertheless, one (1) of the areas deals with the aspect of what could be considered as cyberbullying. The definition of the word "bullying" suggests, for example, that the one (1) who is perpetrating the bullying is obviously more powerful.

They have a greater, whether it be physical or otherwise, capability. The Bill threatens $70,000 fines and up to seven (7) year incarcerations for cyberbullying which includes using a computer system to publish, broadcast or transmit data that is offensive pornographic; indecent; vulgar; profane and obscene. Or, which, I think we all agree and do not think we would disagree with those particular sentiments or, to cause annoyance. We are looking at Section 20. My apologies. Section 20. Or to cause annoyance; inconvenience; danger; obstruction; embarrassment; insult; injury; humiliation; intimidation; hatred; anxiety or causing substantial emotional distress.

I could be standing in my pulpit a Sunday morning preaching a message that does not endorse homosexuality or lesbianism which the scripture said such were some of us; suggesting change is very possible. That could cause some humiliation to some. It may cause some intimidation to others. It may cause some annoyance. What in its broad expression the Bill is suggesting and this is why I am thankful that Mr. Greene referenced the perception. The Bill is suggesting that if I did that, I could find my actions criminalised.

As far as I am aware and stand to be corrected because I expressed I am not a lawyer; once that goes on my record, it is on my record. Would I be correct for those of you who are more knowledgeable? The expansion of the scope on the meaning of cyberbullying beyond specific definitional terms can lead to challenges in interpretation. A review of what acts are considered to be cyberbullying in various jurisdictions highlights that the Barbados Cybercrime Bill 2024, unnecessarily broadens the scope of acts of cyberbullying.

The Bill uses language that combines words open to being deemed as vague, overly broad, arbitrary and/or subjective and uncertain and expands the potential reach of the law beyond what is necessary or clear. I must confess that yesterday I had a debate with two (2) of my children on some of these matters. I found it very interesting, Members of the Committee, that they were somewhat fully supportive of taking action in this area to some degree, especially when one (1) considers that there are some aspects that if they are enacted by an individual can have long-term impacts on a person's ability to be employed; their ability to travel for that matter; their relational components and other areas.

I thought it rather interesting because I raised the point with them where they felt that it was not the

responsibility of the law to police their children but the parents. If an act, I believe there is a limitation in terms of legal action that can be taken against a minor and in the absence of that, the action I would expect to be taken against the adult. They felt that that to some degree and instances was in place because some adults just do not monitor what their children are doing.

As you know, I believe it is right that around 33 percent of the activity on the internet today through social media is done by young people. A lot of that aspect of cyberbullying occurs on the internet. In one (1) instance, I remember in the US that it actually led to the death of a child. This is just one (1) specific area. There are some others that we can touch on.

Mr. CHAIRMAN: Reverend Nicholls, I have absolutely no intention of getting into any debate with you on religion. You would say that I am not qualified to do so, just like how you have freely admitted you are not qualified in law. You have Freedom of Assembly and Freedom of Association, under Section 21 of our Constitution and Freedom of Conscience, under Section 19 which speaks towards freedom of thought; freedom of religion; *et cetera*. It is your freedom of religious expression to condemn homosexuality in every form and you ground biblical context in that.

Others think otherwise. I do not know that this Bill, as presently drafted, is going to curtail you from what you have been doing; you and some of your fellow colleagues Pentecostal

Associates but surely I have to ask you, if you were to go say on the pulpit next week Sunday, *"I hate homosexuals! I feel that all of them should be killed! Kill all homosexuals!"* Do you think that you have the right to say so because you have a constitutional right to Freedom of **Conscience** and Freedom of Association and Assembly?

Though you do not agree with homosexuality, that you can within the context of the Cybercrime Bill. Right now posts on a computer that all homosexuals practicing and otherwise closet, open whatever should be killed. They have no right to be living in this country and they are an abomination in the eyes of the Lord. You feel you have the right to say so?

Rev. Dr. Ferdinand NICHOLLS: Mr. Chairman, I believe the Budapest Convention addresses matters of xenophobia and that is from that perspective but since you are asking me, the personal question that would be a betrayal of what I believe. When one considers as I mentioned a moment ago there is actually a biblical verse that references the fact that such were some of us but we have been washed. We have been justified. We have been sanctified so for me to stand in my pulpit and promote hatred of any entity whether it be persons of gender; race; colour or otherwise, is inconsistent with my faith.

I deal with a Lord who came into this world because he loved. It can often be seen that when one is objectionable to a matter, that they automatically hate and that is not necessarily the case. We can disagree but our disagreement does not necessarily mean I do not like you or I hate you. I disagree with your view on Freedom of Speech and Freedom of Expression but my relationship with you will not change and so, I have to be committed primarily because as I sat here, I said to you and the Committee. I sit here as an Ambassador for the highest government that we know of and I am committed to that government and incidentally, I am not speaking on the behalf of the Pentecostals or the Pentecostal Assembly or any other religious denomination in Barbados; so I would be betraying my faith, if I was to make a comment like that.

Mr. CHAIRMAN: Yes, Mr. Nicholls.

Senator G. P. B. NICHOLLS: Yes, I would like to congratulate Reverend Nicholls for those honourable sentiments just expressed. I was not sure Mr. Chairman, if your off the wall example does justice of what already a substantive matter. I know sometimes that is where the popular discourse goes into the heat of the matter and we bring out extremes but I would appreciate if Reverend Nicholls were to give us some clarity. I know he gave that example but I am clear in my head that Cyber Bullying does not prohibit or the law as intended against Cyber Bullying, does not prohibit any pastor or any person speaks to matters of conscious in this society and that **was carried live.**

I tend to do a little research and I have fallen in love with Lord Sumption. Mr. Thorne would know him, who was on the United Kingdom (UK) Supreme Court recently. Very strong advocate for the fact that the entire world wrongly curtailed fundamental rights in the COVID-19 era and it was an overstretch and not saying that we did it wrong or anything like that but I do recall him saying recently in one (1) of the lectures at, I believe at Oxford University, that people should have the right to say things that are objectionable. People should have the right to say things that are abhorrent and you cannot silence someone just because you find what they are saying objectionable or abhorrent.

We have traditionally drawn the line and I am just paraphrasing from him, that where that abhorrent objectionable statement is likely to cause danger to life and limb. That is where the law has necessarily drawn the line but we are to be careful that we are not in a rush to silence all speech just because we do not like the content of that speech and again I want to assure you and I think you know me long enough and you know me well. I cannot see any court in Barbados, of which we are under its jurisdiction, with our apex court being the Caribbean Court of Justice (CCJ), that would allow any state under its jurisdiction, to pass a law that would do those things that you have so legitimately brought to our attention and concern and I have said it in the first meeting that we have had.

The vague language that the Bills are being accused of is something that we have to look at it and I not necessarily feel that we could throw out the baby with the bath water because I had a conversation with a school mate of mine who is in the security system regionally and I made that comment here and the level of interference with children and those of us who are in the legal profession and counselling, Sir. If Bajans knew the level of interference by adults with children and the exploitation on the internet that goes on in

this country; it would be shocking and as a parent, I feel as again, as I said in the previous speaker.

Parliament has to pass the laws and we have to debate them and these sessions are part of the new structure going forward in the Republic and we have to debate these in Joint Select Committees and invite the public to comments as the Bills are going through their Parliamentary processes, yes. It is going to be a messy exercise but let us not hate one another in the argumentation of the various views that have to contend in a democracy.

We have to tolerate views that are not in concert with our feelings and why? The minority of the society live in the society and they enjoy the rights as well. It is not the majority who get to say what the rights are. It is the benefit of all in the society; even those who are on the fringes of the society and we have come too far out of those fringes, when all of us would have in times of the past may not have had the right to be in this building; in this room at this time having a say on national issues. Certainly 60, 70, 80 years ago, it would have been unheard of.

We need to understand and appreciate that not everyone is going to share our views and you have to except criticism within the context but at the same time, it does not mean it is the wild, wild west. It is a licence for all. I am aware and it is last my comment, I said this before Mr. Chairman but I say it for the benefit of Reverend Nicholls. Of suspected suicide by way of Cyber Bullying going on in Barbados last year where it was very prevalent. Suspected. Not for the reasons my friend would suggest, otherwise but this is something that concerns me as a parent. Let us engage and let us get this process right and the Bill will not be perfect the first time but at the same time, they are means of moving it to a more perfect balance. Thank You. So I just wanted to share that with you Reverend Nicholls. Thanks.

Mr. CHAIRMAN: Honourable Opposition Leader.

Mr. R. A. THORNE: Thank you very much, Mr. Chairman. Reverend Nicholls, immediately preceding your appearance was the Head of a very significant media organisation in Barbados. We can call him a leader in the media and you are a leader in the church. Those are two (2) very significant social institutions, if you do not mind me referring to the church as a social institution, which it is. There are reservations coming from both of you and I would take it that his views and your views are representative of the institutions from which you come.

I wonder if the Government and this Parliament would wish to ignore the reservations expressed by those two (2) very significant social institutions.

I am not going to make a speech. I have said elsewhere and I will say it here that not every aspect of legislation can be condemned and when you find your significant social institutions rejecting what Parliament is doing, simultaneously, if you find that there is a time at which these institutions. Are you with me, Reverend?

Rev. Dr. Ferdinand NICHOLLS: Yes.

Mr. R. A. THORNE: One begins to wonder if it is not a question of trust. While we say that not every aspect of legislation is subject to condemnation, yet you hear the condemnation from these two (2) very significant institutions. That is my question to you. Is the question of a lack of trust, a part of your objection? That is not a long hop in case you play cricket.

Rev. Dr. Ferdinand NICHOLLS: Thank you for the observation and the question. Since this pandemic has begun that we have just passed through; the matter of trust of governments globally has been an issue for every single citizen. When we began this pandemic, we were told that much of what highly expert; highly reputable professional individuals expressed concerning the pandemic, was misinformation and false information. That was equally applied to the treatments that were mandated by governments. Where today, just today AstraZeneca has admitted finally that their treatment has serious side effects.

We were saying that from the beginning. I remember watching an interview with an administrative individual of a particular country, which I will not reference, in which they told the interviewer, we need to control the information that is going out, when the persons will be promoting misinformation and false information were governments and the mainstream media. I make no apologies when I say that there are certain international agencies, again which I would respect, that are complicit in that action.

The European Union (EU) has established a committee, specifically to investigate the pandemic and the after effects of the treatments that has proven that every single thing that was sent prior to by the very man that mandated and brought out the treatment itself was correct. As a

result of all of that, when you put all of that together for the citizens of a country, governments period, have lost the trust of their citizens.

That is not in doubt. If you go to Spain; if you go to Italy; if you go to the United Kingdom; if you go to the United States; if you go to Australia; if you go to New Zealand or if you come to Barbados, you find that trust is at a very low level.

Now, from a ministerial standpoint, trust is an extremely difficult thing to repair once violated and it takes time and it takes admission of failure in order to begin that process. The previous contributor mentioned the matter of communication. Many years ago, I was sitting on a marriage seminar in which the minister spoke of the fact that communication was the roof of the marriage. In truth and in fact, in any relationship communication is key.

When communication is found not to be true, you have a major crisis on your hand at every relational level. That is a problem we have had over the last three (3) to four (4) years. It is known beyond a shadow of doubt. The Prime Minister of Canada is currently facing serious legal ramifications as a result of his autocratic mandates in Canada. It is there for the whole world to see. As a result of that, I do not know if you can call it a trickle-down effect; where people simply now do not trust. If you ask me how Government can repair that, it has to start with being transparent.

Mr. R. A. THORNE: No, I am not asking you that.

Rev. Dr. Ferdinand NICHOLLS: You are not asking me that.

Mr. R. A. THORNE: No.

Rev. Dr. Ferdinand NICHOLLS: You want me to hold onto that. I will make that a part of my campaign.

Mr. CHAIRMAN: Reverend Nicholls, we are here to talk on the Cybercrime Bill. If you do not have anything else further on the Bill.

Rev. Dr. Ferdinand NICHOLLS: No Sir, I was just responding to your Committee Member's question.

Mr. CHAIRMAN: We thank you for your contribution this afternoon and for accepting our invitation.

Rev. Dr. Ferdinand NICHOLLS: I thank you for granting me the honour and privilege. Thank you and thank you, Committee.

Mr. CHAIRMAN: I would have wanted to proposedly go through. Mr. Stuart has been here from the beginning waiting patiently. We now invite you to come forward and give your oral presentation. Reverend Nicholls, you are free to submit what you read to the Committee.

Mr. Stuart, welcome, you were here from the beginning and you heard it all, so I do not need to repeat to you the rules of engagement for you. You have your laptop, so you are free to submit whatever you have in writing even though it is an oral submission. In fact, I would advise you to present it to the Committee. I know whether you should submit a written presentation, in addition to oral was a debate and some concern and you did say that you will be willing to submit whatever you are saying in writing. I invite you to if you wish. You have 10 minutes, Sir.

Mr. Kemar STUART: Before I start to utilise my time, I just want to say good evening to you, Mr. Chairman; good evening to the entire Committee; the Leader of the Opposition and to the Members of both Houses. Good afternoon to all Barbadians and to those persons who are watching my name is Kemar Stuart; I was invited as an individual, so I am here to represent the self in an individual capacity. I will state for the record in my professional capacity, that I am a non-resident research fellow at the Caribbean Progress Studies Institute. The views this evening are mine and not that of the institute.

My first observation, quoting from the Bill, specifically Part III which deals with Investigation and Enforcement. I am going to reference some words that are in the legislation. These are insults, embarrassment and humiliation. I am going to say that it is my perception that those words are very emotive. With all good intention, you can post something on social media, well-intentioned but caused the same effect, as though you did it unintentionally with the aim of being reckless. Who is to determine if you are punishable by the court of law?

Secondly, it is my concern that this Bill empowers the Police Service of this country with extraordinary powers. I say that because when you speak about search and seizure or the section that deals with search and seizure specifically and again, I am reading from the legislation; it is nothing I would have prepared.

It states, *"Where a judge or magistrate is satisfied, on information on oath given by a police officer, that there are reasonable grounds for*

suspecting that an offence has been, is being or is about to be committed in any place and that there is evidence that such an offence has been, is being or is about to be committed in that place, the magistrate may issue a warrant authorising any police officer to enter and search that place, including any computer system, using such reasonable force as is necessary."

My criticism there would be, how would the police know that a crime is about to be committed unless the police were indeed actively monitoring the citizens of Barbados? My next question would be, if indeed the police are the ones to oversee or has the authority to execute the offences in the Bill, what resources do we have in terms of a Cybercrime Unit to be able to man the offences in the Bill? I heard earlier by a presenter that the Bill is likely to cause a ripple effect in terms of the numerous amount of persons that could be potentially held liable.

Do we have the resources within the Police Service in terms of staff, qualifications and otherwise that would equip them to carry out the requirements of the Bill? My next observation here would be, why only the Police Service and not the Barbados Defence Force (BDF)? Outside of that, you have in other larger countries security agencies or private security agencies. In this specific legislation, it speaks to an appointed person and this appointed person could be empowered or imbued by the Commissioner of Police. Either the police themselves or somebody who has knowledge of a computer system or otherwise that they could instruct to assist.

A prime example, we had a situation in Barbados where we had a former Commissioner of Police of Barbados who had specific skills and it was public knowledge that a former Commissioner of Police of Barbados was indeed sent on retirement based on recommendations from the Police Service Commission. I will enter into the record the specifics of the charge but it relates back to my original question of actively monitoring Barbadians and internet traffic. It includes all types of traffic; phone logs and pictures. In the Bill specifically, it empowers the police to engage persons who have the necessary equipment to do decryption.

On WhatsApp, one of the most important or attractive features is security and that you are not able to decrypt my messages. It is one (1) of the benefits of having WhatsApp. If a country is attempting to bypass a big technology firm because WhatsApp is no small firm, that is not based in Barbados, you are looking for legal trouble. We speak about that and I am going internationally because the next part of my presentation deals with the Mutual Assistance in Criminal Matters (Amendment) Bill.

That Bill originated from the 1980 Mutual Assistance Act to deal with criminal matters. The amendments being discussed here today deals with mutual assistance as it relates to computer-related crimes. Before, the application of that Bill spoke specifically to Commonwealth countries; countries that were signed on to the United Nations (UN) War on Drugs and Crime. As of late, the new amendment says, *"with any other country that has signed on to the Budapest Convention."*

What is so special about these additional countries that will be added to the list, where information sharing will be occurring between Government to Government? In the Bill, there are clauses which speaks to confidentiality of requests between the two (2) countries.

The esteemed gentlemen on my right and immediately to my left, they are all politically affiliated persons. In the Bill, it speaks specifically to crimes of a political nature and it lists the crimes that would not be considered to be a political crime; why not create a section in the Cybercrime Bill which speaks specifically about criticisms of public officials and what is allowed from what is not allowed, to give the public a sense of confidence, that public actors and officials are not abusing State power to shield themselves from criticism?

I say that in the context that we have a 29 to one (1) in the House. Before, it was 30 to 0 twice. How are we, as a public to perceive a State, having a lopside and serious imbalance of power and then you are attempting to criminalise free speech in a way where the voting estate which is not elected, you want to regulate their speech? Parliamentarians, have cover in parliamentary privilege. Meaning that, any of the gentleman on my left or right could get on the floor of Parliament and criticize; insult; embarrass or do whatever and have parliamentary coverage but I do not.

The one (1) area I have which is freedom of expression which is social media, then you attempt to regulate it and over regulate it to the point that you have actually gone pass the security measures that the big technology firms; the same

persons who made the applications that we use, you want to over-regulate it more them. Right. Those are my general concerns there. I want to come to the end of my presentation soon because I do not want to go on extensively.

The last part deals with Section 25 because I think I dealt with the encryption information and allowing persons who would decrypt data. It says record of seized data to be provided to owner. It says, *"Where a computer system or computer data has been removed or rendered inaccessible to the owner"* and the police under the Bill has the power to render your devices that they confiscate inaccessible to you. It is saying here that:

"the person who has control of the system following a search or a seizure under Section 23, the person who made the search shall, at the time of the search or as soon as practicable after the search:

a. make a list of what has been seized or rendered inaccessible, with the date and time of the seizure; and

b. give a copy of that list to

i. the owner of the computer system or computer data;

In the next breath, it says that under Sub-section (3):

"that a police officer or an approved person may refuse to give access to or provide copies of computer data referred to in Sub-section (2) if he has reasonable grounds for believing that giving the access or providing the copies

b. would prejudice

i. the investigation in connection with which the search and seizure was carried out;

ii. another investigation connected to the one in respect of which the search and seizure was carried out."

This means that if you take away my devices in a search and seizure and I am cleared; if a policeman decides to get overly emotional and petty, he could say that he is keeping my devices and this law allows him to do it without recourse or without stipulation. Send to the police how long you could keep my devices for, the same way you would treat a person or individual who comes into contact with the law. There is a set time that you can keep an individual in a police station without formally charging the person or committing them to be answerable to the Magistrate Court or whatever court there is, so the same should be with this.

It says here they believe:

iii. "anymore criminal proceedings or that may be brought in relation to any investigations."

Mr. CHAIRMAN: Mr. Stuart, one (1) more minute.

Mr. Kemar STUART: My question is, if you believe that the first charge was not successful and you go back to the drawing board and you believe that you want to build another case against me, you continue to keep my devices and pass laws to preserve my data, that I cannot even swipe or **clean** my own property, that I bought with my own money. That has nothing to do with the State but it was a private purchase and the State of a country should not be depriving the citizens of their private property in that of a phone and if the government wants to engage apps and traffic data and web data; the best thing to do is to engage the big tech firms like Whatsapp; Facebook; Telegram whatever, as oppose to overreaching as it relates to empowering the police with extraordinary powers, for a job that we do not know if they have the requisite knowledge, skills or experience to handle. Thank you very much.

Mr. CHAIRMAN: Thank you, Mr. Stuart and we now invite Committee Members if they wish to engage you. Okay. If none yet Mr. Stuart, I made some notes. Section 19 (3) and you know you had concerns about that section saying that effectively and correct me if I have misinterpreted you; that you should be allowed to ridicule; embarrass them on social media and you might do that with intention or without intention either way and find yourself subject to the criminal law. Am I interpreting you correctly?

Mr. Kemar STUART: No you are not.

Mr. CHAIRMAN: So explain and clarify what you said there on those issues. When you spoke about ridicule and embarrassment.

Mr. Kemar STUART: In a well-intentioned post, without malice you can cause humiliation; embarrassment; or any of the other emotional words that were used with a well-intentioned post. That may be true but it causes the same effect as though you did it with reckless intention, so who is to say or who can speak to my intent for posting it, when I tell you it was good but you are trying to suggest that it was bad although I said that it was good? Then I have to come to court to prove that my intention indeed

was not sinister but more positive. That is my interjection.

Have you read Section 19 (5)? Have you fully read the section, Sir? Three (3) says whether you have made this post which causes embarrassment or ridicule but you do not care whether it is true or false but Section 19 (5) gives you defences. In other words, if it is true, you can prove that it is true, you get off but suppose someone because they do not like Mr. Kemar Stuart for whatever reason or Mr. Edmund Hinkson because I am not personalizing it and because of that, to get at you or Edmund Hinkson they say something bad about your mother or my mother. They are prostitutes to get at us; you or me. They cannot prove that it is true and to use your words, the intention, they could not care less whether it is true or false. Are you saying that Kemar Staurt, his mother; Edmund Hinkson, his mother; should have no redress? Should not go and make a complaint to the police but this person for whatever reason political or otherwise, has said my mother or in the mother's case, I am a prostitute; it is not true. Are you saying they should have no redress? The police should say 'too bad'. A person can say anything they want about you maybe just because what did you say because they are a public figure; because I am a Member of Parliament; because you are a public figure of sorts; a former General Secretary of the DLP.

A person should be free to say anything about you or your mother and there is absolutely no truth in it just to embarrass you or ridicule you. Are you saying that that is how the laws in Barbados should operate, Sir and would you be happy in that situation; that you your mother or in my case Edmund Hinkson, my mother, has no legal redress whatsoever and persons should be free merrily to go along to say that about your mother or my mother and obviously, we know the situation is forwarded many times. It goes out to whole world repeating it. Repeating this falsehood. Time and Time again, just to embarrass you because you are a public figure of some sorts or me because I am a Member of Parliament.

Mr. Kemar STUART: Your interpretation of your examples, I mean, it will invoke some emotion; a lot of emotion because you are speaking about a female. That is my Queen, my mother and I am assuming your mother would be your Queen so it will invoke an emotional response at first but this is not an emotional place. I started by saying that those words of humiliation and embarrassment were emotional words.

Secondly, the laws in this country under the Defamation Act provides coverage already as it relates to those examples that you just gave so it would not fly. There is no need to overly regulate and let us be honest; that comment can no way be taken in kind spirit at all whatsoever; any comment like that. As a police officer, fresh out of school, still very young, masculine, aggressive, very interested in proving to his superiors that he can make it up the ranks. He has to sit and determine for himself if this statement that he is looking at if it merits him making an approach to go and convince the magistrate to go and get a warrant to come and charge you.

This police officer is looking at this statement about my mother. He has to consult with his superiors before he does anything. My question there would be; not to drift to far from the point. My answer to you would have been, "No! I would not like something like that to happen." If a Parliamentarian is afforded free speech with parliamentary privilege and coverage, I am saying that the public should be afforded that same right within measure, and if you want to regulate the public, you have to regulate yourself. This is where I agree with Mr. Greene from STARCOM Network, that a Freedom of Information Act should on the table as oppose to a Bill to …….

Mr. CHAIRMAN: Mr. Stuart, we are not talking about Freedom of Information legislation.

Mr. Kemar STUART: Yes but you have to give to get.

Mr. CHAIRMAN: I need to be clear, Sir, do you accept that Section 19(5) provides a defence, that if what you say is true, it is public, in the public interest they say so, you have a defence. Whether you already have defamation legislation which provides a defence or not, do you accept that those defences, truth, comment, triviality and privilege, absolute or qualified, provide a defence to what somebody says about you or the examples I gave, your mother, my mother, even if they embarrass you, your mother, my mother or myself. Do you accept that there is a defence and that somebody who says that is covered?

Mr. Kemar STUART: I am not sure because the way how you craft it. I will go back to the example of a police officer. That young masculine, aggressive police officer has to

determine first and foremost if an offence has been committed based off the legislation and if indeed that the matter is trivial as you said; the matter is truth as you said and it speaks here about provided for under the Defamation Act.

If the Defamation Act covers your question, then the Defamation Act stays and the Defamation Act will be my point of reference as well. When you go much further than that, outside of the scope of what is provided and it is true, if I speak the truth, I should not be charged or I should not be prosecuted; I should not be harassed in any way, as long as what I am saying factual and truth and I can back up my statements with written or video evidence.

Mr. CHAIRMAN: Yes. Where in this Section that you have quoted does it say otherwise? Since the defamation defences apply to this section, where in this section that you have spoken about, is it contradicting what you have just said?

Mr. Kemar STUART: If it contradicts what I just said?

Mr. CHAIRMAN: Yes.

Mr. Kemar STUART: Yes.

Mr. CHAIRMAN: Whereas you speak the truth, you do not get off.

Mr. Kemar STUART: You said it and you quoted from the legislation. If you post this video, whether you know if it is true or not, it is right there in the legislation. I want to go back specifically to quote it because I do not want to paraphrase Mr. Chairman, so let me capture it here please. I think it was under the cyber bullying section where it speaks to being true or not.

Mr. CHAIRMAN: Do you have it there?

Mr. Kemar STUART: I am trying to find it; it is right here.

Mr. CHAIRMAN: You were talking about Section 19, Mr. Stuart and you have now moved on to Section 20. You seem to have concede that what I have said you have no answer to because you have now moved on to cyber bullying. Let me hear what you are going to tell me about cyber bullying.

Mr. Kemar STUART: I have not moved on. All of these are offences, at the end of the day it is an offence, so you have to face the same punishment, maybe a little more money or less money in some instances but it is still an offence. I want to take the specific reference in the legislation, which says, if you post this thing believing it to be true without knowledge as to if it is true.

It says here at Section 19(3):

"*A person who intentionally uses a computer system to disseminate any image or words, not caring whether they are true or false, and causes or is likely to cause or subject a person to ridicule, contempt or embarrassment, is guilty of an offence and is liable on summary conviction to a fine of $70 000 or to imprisonment for a term of seven years or to both.*"

If I go by your reference, you are saying to me that only this specific Section, which is Section 19, if I publish something whether true or not, I can only be charged under the offences specifically listed under Section 19? Is that what you are saying?

Mr. CHAIRMAN: You have come to tell me, Sir. What I am saying is that I see in Section 19(5), a defence, not saying that you cannot be charged. You know a lot of people that have been charged and were found not guilty. Section 19(5) protects you, does it not?

Mr. Kemar STUART: If I speak the truth in the first place, then I can come back with the truth as a defence? Why do I have to go through the public ridicule for speaking the truth in the first place that a police officer can take it upon himself to come my house; seize my laptop; my computer; my devices. I am taken to a police station, bear in mind I have not spoken yet and the police engage you. You have to go to court, spend money by hiring a lawyer, do all of these things to prove.

Mr. CHAIRMAN: Mr. Stuart, we do not live in a perfect world. We are all men on this Committee and you are a man, you know very well Sir that tonight, anyone can lay a charge against us, sexual assault for example, so what are you saying? What are you telling us here? It might not be true and the police come for you base on that allegation. What is the difference between that and this? I really do not get you.

Mr. Kemar STUART: Let me give you an example that is close to home. I will not speak because of sub judicate, so I will not speak in details. Let us just say a scenario occurs like sexual assault as you said and this person happens to carry a public position. I saw in real time and real life, where information was put on the internet purporting to the information originating from the Barbados Police Service. Whether this

information was true or not; the facts were put out there. This person has to go through the courts.

Mr. CHAIRMAN: That is subjudicate but you essentially agree with me.

Mr. Kemar STUART: I am essentially saying that if this person has to go through a public ridicule, based on false allegation because it is the police officer who lays the charge, so that person has to determine whether or not to proceed after a complaint is laid, I suppose. Nothing like that was said here. This person has to go through that scorn. If that person is found not guilty which is the person accused, what happens then? What happens then? You are then back to square one when lost all of your public credibility on a false allegation.

Mr. CHAIRMAN: Are there any other Members who wish to intervene and ask Mr. Stuart anything? Mr. Stuart, you raised one (1) good point. You asked who would police this in the Police Service. Again, that is not the concern, you could appreciate, of the legislature. The legislature passes laws. It is up to the police to decide how they will monitor or implement the law or *"police"* the law. That cannot be a reason for not passing the law. You could appreciate that. I just came back from Trinidad this morning. When I asked, yes, their police department has a separate Cybercrime Unit to deal with.

Sorry, not Trinidad, Guyana. Guyana has passed the law; Trinidad has not passed it. I was told that Guyana has a separate Cybercrime Unit to monitor and enforce the law but that is not Parliament's role. You concede that? Okay. Police excessiveness; you spoke about the police having the power if they suspect a crime is about to be committed to pursue it. Is that not so with other laws as well? Cannot the police, for example, stop a vehicle tonight that they feel may have occupants in it who they have received information may be going to commit a crime or involved in a drug bust or not? What is do different with the legislative provisions of this Bill, as drafted, to existing law?

Mr. Kemar STUART: Your first comment about policing, my grave concern there, you said it is not a reason to pass the legislation. My grave concern stems from the fact that our Westminster system and particularly the Mutual Assistance in Criminal Matters Act of 1980 names the Attorney General as the central authority, as it relates to mutual assistance in criminal matters. By origin, the Attorney General is a person who first and foremost is a member of a political party. Secondly, he or she is a Member of Parliament and then, you are elevated that job at the courtesy of the Prime Minister.

The Attorney General, being the central authority and bias in that he is a politician who is a member of a political party and by the fact the Prime Minister, who that person serves at their behest, follows something called collective responsibility. Upon instruction, the Police Service can become politicised to the point that it can be used to enact witch-hunts on people based off the directives coming from the central authority. The last comment you said, could you remind me quickly?

Mr. CHAIRMAN: Police having the authority to intervene where they suspect a crime may be about to be committed.

Mr. Kemar STUART: The example you gave is that of a physical nature; flesh, bloods. We are talking now cyber. That is the reason it is called the Cybercrime Bill. The reason it is called the Mutual Assistance in Criminal Matters as it relates to the computer. How would you know that I am sitting here on my device planning to commit a crime unless you were actively spying or monitoring my device? If any community member could say, "How would you know that a crime is about to be committed on a laptop or tablet?" You must be seeing it. If you are not doing the spying yourself; you have to be engaging the service provider like Lime, Digicel or AT&T.

There are clauses in this Bill which speaks to that. My fear here is that the telecommunications companies can be intimidated and bullied into sharing the private information of the public, based off the structure of our current political system.

Mr. CHAIRMAN: Unless there are any other Members who wish to intervene with Mr. Stuart; Mr. Stuart we thank you for your presentation. Pursuant to your request for oral, we thank you for coming.

Mr. Kemar STUART: Yes. Thank you very much.

Mr. CHAIRMAN: This brings us to the end of our public hearings for today. We would invite the public to leave and just deliberate on a few matters. We thank you all. I want to detain you for few more minutes to go back to the agenda. Minutes of our last meeting. Did you get a chance to read them?

On the motion of Senator G. P. B NICHOLLS seconded by Mr. P. R. PHILLIPS, the minutes for the meeting of Monday, April 22, 2024 were confirmed.

Any matters arising? For the record, Senator Nicholls and Member of Parliament, Peter Philips. Matters arising under these Minutes? Any matters arising?

Senator G. P. B NICHOLLS*:* Mr. Chairman, there are not a lot of extensive Minutes. There are one (1), two (2), three (3), four (4). There are six (6) items. We are talking about matters arising, so I am just saying…. When we look at the Call to Order, Minutes of the last meeting, Matters arising from that meeting, Consideration of the Bill and Any other business.

Mr. CHAIRMAN: Hence, no matters arising. Under Any other business, I would have sent Committee Members a list and I am not so sure if everyone would have had a chance to read all forty-three (43) of the submissions. I mean so

we were really short. One paragraph and then some were saying they would like to come to give oral submissions but you would see that I would have siphoned out 12 of the written and then the four (4) others who said that they would like to give orals.

In other words, everyone who said that they would like to give orals, I recommended that we give the opportunity to come and give oral for the sake of transparency, accountability. I do not want anyone saying that they asked to come to give an oral and we did not allow them and then out of those who gave written, I have identified 12 persons to come and give evidence so I would wish to hear the Committee Members comments, if you agree.

Senator G. P. B. NICHOLLS: Mr. Chairman, how many people would that be?

Mr. CHAIRMAN: Seventeen in all. I think it is because I had 10 and then they had two (2) extras and four (4), so 16 in all out of the 43 and included in the 43 there was a petition signed by quite a few people about three (3) pages of names. I cannot say signed; the names were on. No signatures. I just need your comments on it. If you feel that is too many. If you feel that is too little. If when you read them, you agreed that these are people who can contribute and assist us in compiling a report.

Senator R. O. WALTERS: Mr. Chairman, I think it is the right thing to do especially the ones that requested them to submit orally and besides the additional persons. They are 17 persons in all. I think we should see everybody so that the issue is well ventilated and persons get a chance, Sir.

Mr. CHAIRMAN: You mean the 16 that I have identified?

Senator G. P. B. NICHOLLS: Sir, I differ from my colleague and friend. I feel like if people have not requested to come and make oral presentations that we do not need to bring them. Let us hear the ones that are oral so we can have an opportunity to discuss amongst ourselves the content of those submissions because we still have to find time to discuss them amongst ourselves as a Committee, so as to do the report and that I fear would delay the process. If someone has written to us and submitted something in writing, why would we ask them to come? I understand the people who came today and why that was selected but I do not agree.

Mr. CHAIRMAN: Okay. Let me expand a bit on my reason and like I said realise under these rules I do not have a vote. All I have is a vote, if it is three (3) all.

Senator G. P. B. NICHOLLS: I understood what you said.

Mr. CHAIRMAN: No, I just want to expand like Ms. Maureen Holder. She specifically speaks in terms of Consumer Protection under this law, so she is unique in that sense because other talking about Freedom of Speech and things so that is why I identified her. David Weekes, I do not know. I am neither here or there. Chesterfield Brown, he claimed to be very knowledgeable so I send him. Cammie Holder, we all know Cammie. Cammie is an activist so I said look give him the opportunity to come.

I am trying to be and I do not want us at the end of the day to be criticised and someone to say as has been said, that this is just a sham. We will get criticised anyhow. Mr Peter Lawrence Thompson; he wrote posts on it and in fact, Sir David if I recalled would have drawn reference to what he said. I may be wrong but certainly he gave comments ion the Parliament website under the Bill. Mr. Grenville Philips; I do not have to justify why I put him and Senator Walters has said the four (4) others listed below, they asked to give oral evidence so I put them in.

As I said, we can vote on it if Members do not agree with all 16 and I would propose; we took longer with Mr. Steven Williams and Mr. Niel Harper because they gave bigger written submissions. I do not propose that these persons, 16 will take as long a time and I would propose two (2) other sessions to hear all of them; if Members so agree. I am open to you all, as I said I do not have a vote in this. It is my duty as Chairman to propose but could be rejected.

Senator G. P. B. NICHOLLS: Mr. Chairman, my challenge is the luxury of time. We are also in the process of wrapping up the business of the Constitutional Reform Committee. We have to find time to meet with the Leader of the Opposition and one of the reasons why we did not meet in the last couple weeks is because we were dedicating our time to this here and we do not have luxury of time. We also have to meet with the Parliamentary Reform Commission as they wrap up.

Mr. CHAIRMAN: I understand that they are sitting Wednesday; Thursday; Friday this week but I am conscious that Senator Nicholls. I do not want anyone to say that this Committee was a sham. It was just set up. We were given three (3) months; that is the next thing. The Senate gave three (3) months not the Upper House, the Senate on 08 February, 2024 which expires next week or was 16 February, 2024; that expires next week. We only started on 08 April, 2024.

In other words, we started less than a month ago, so in any event we are going to have to ask the Senate for an extension because of the change with the Honourable Member for Christ Church South and obviously, his Constitutional right to appoint Senators, we started late and I suppose the Senate would have to understand that but I will propose but this is for a decision to ask the Senate to extend our mandate to the end of June, which would still be within a 90 day period from when we started on 08 April, 2024. I do not want anyone to say that we rushed through and they were not given an opportunity to be heard. Granted, these 10 did not ask to be heard and we can take what they wrote but if there were any of the 10 any Members, having read what they submitted felt that we need to hear them further on; I was given Members that opportunity. If the feeling is do not worry, let them stand by what they wrote as I said, it is for you all to vote. I do not have a vote.

Asides.

Dr. R. O. SPRINGER: What we could also do if you have curated the list of 16 or so, we would have persons come in and speak to certain aspects of the Bill. If it is Section 19, 20, Section 11 and you have three (3) or four (4) persons speaking to that, it makes no sense to hear all three (3). Once you have curated the list.

Mr. CHAIRMAN: That is why I have identified these 10 out of the 43.

Dr. R. O. SPRINGER: I know you have listed some.

Senator G. P. B. NICHOLLS: Sir, I do not want it to be said that we are trying to short circuit the process. I have already spoken to my colleagues in the Senate and I am sure Senator Nurse would agree that we would have to ask the Senate to extend and we are prepared to make that move. For me, the more important thing is for us to have a discussion amongst ourselves as to what the public submissions are, to see if we can reach any consensus because I gather from Sir David's presentation that they are areas in which the drafter would have to do some tightening of the language to deal with the issues of the vagueness and the uncertainty in terms of what is a criminal offence and what is not.

Also, where we are now creating statutory offences outside of the Budapest Convention that we are making sure that we are not overreaching. Those are things that have already see as broad, having agreed that the drafter could come back. We have to discuss the meat of the matter as a Committee, to make recommendations back to our Parliamentary Colleagues as to whether the Bill ought to be amended or whatever but to me that is the more important part of the work.

Asides.

Senator G. P. B. NICHOLLS: I am just saying public submissions notwithstanding, they are in writing and I am not trying to stop anybody from coming on any given daybecause this process is not going to end in a hurry. I do believe that we are not sufficiently taking the time to go through the public submissions because I do not know if we are gaining a lot from what is happening here. You give them 10 minutes to come and say something and there is a back and forth, but what is that? I mean that will ensure

that no one cannot criticise you but I am more of a substance man, so I want to read the things, I want to study them and I want us to discuss them.

Mr. CHAIRMAN: That comes at the end of the hearing. Certainly, when we finish these oral hearings, we will get together because we have to submit a report.

Senator G. P. B. NICHOLLS: I am saying that we can discuss submissions that came in at a meeting and then from that discussion, we could determine whether or not, based on our uncertainty any questions that we want, whether we want to invite that person to come in, rather than doing it the other way. That is just a suggestion.

Senator R. O WALTERS: At a bare minimum, we should see the persons who requested to see us. It is four (4) that I have identified.

Mr. CHAIRMAN: The four (4) plus Roslyn Corbin, so it would be five (5).

Senator R. O. WALTERS: You made a point about an organisation like the Barbados Consumer Empowerment Network.

Mr. CHAIRMAN: That is why I said Maureen Holder.

Senator R. O. WALTERS: I think if you have similar organisations like these that are questioning other things other than what we have already heard, I think they should have the opportunity to also present.

Mr. CHAIRMAN: Alright.

Senator R. O. WALTERS: It might not be 10, it might end up at four(4).

Mr. CHAIRMAN: Okay, like I said, Mr. Grenville Phillips, we all know who he is. Mr. Cammie Holder, always claims to represent certain interests, so does he fall into the category that Senator Walters is saying?

Mr. P. R. PHILLIPS: Mr. Chairman, it is not who …….

Asides:

Mr. P. R. PHILLIPS: I am reading all of these submissions that were delivered by Parliament and I think that having read those, we should all look at them and then from then support the point Senator Nicholls have raised.

Mr. CHAIRMAN: I read them, so that is why I took them out.

Asides.

Mr. CHAIRMAN: I think the consensus is that we hear the five (5) who have asked for oral submissions. Is that a minimum consensus? Okay. Do we add Maureen Holder to that, because as I said, her paper is on consumer issues, whether the consumer is protected in this Bill, which is unique, out of all the 43. Do we add her?

Senator R. O. WALTERS: I believe so.

Mr. CHAIRMAN: Hear six (6) people in the next occasion. Do we agree with that? Or, do we just hear the five (5) and leave out……

Asides

Mr. CHAIRMAN: Yes, we are going to come to that.

Senator G. P. B. NICHOLLS: I am saying we have to organise our business now.

Mr. CHAIRMAN: Yes, we are doing all of that and definitely as I said, we have to ask the Senate for an extension. Do we agree on the five (5) or the five plus Ms. Holder?

Mr. CLERK: Mr. Chairman, there are seven (7) persons who have actually requested that they want to give oral presentations.

Mr. CHAIRMAN: I counted five (5). Is it seven (7), including who came today?

Mr. CLERK: We did five (5) today.

Asides.

Mr. CHAIRMAN: Phillips wrote. We are talking about people who said, "*I want to give an oral presentation"* but they did not submit anything in writing.

Asides.

Mr. CHAIRMAN: He submitted in writing, so there is no consensus among members that you could write in which is what Mr. Phillips did and say as well, I still want to give an oral presentation.

Senator G. P. B. NICHOLLS: I am saying let us have a look at it before we make that decision.

Mr. CHAIRMAN: I am talking about for the next time. I think we have agreed that those who give oral presentations with no written submissions, we should hear them. As I understand that from when I looked, there was Janine Butcher; Victor Lewis; Heather Cole;

Timon Howard; and there was Roslyn Corbin. That is five (5).

Mr. CLERK: There were five (5) who requested oral submissions.

Mr. CHAIRMAN: Which five (5)? Those five (5) that I just named?

Asides.

Mr. CLERK: Janine Butcher; Victor Lewis; Roslyn Corbin; Heather Cole and Timon Howard.

Mr. CHAIRMAN: Right, those five (5). I think the consensus is that we hear those five (5). Who said that they want to give oral presentations but did not give written submissions. In other words, at this stage, we are not including Mr. Grenville Phillips because he gave a written submission and we can read his. Obviously, I understand Members may not have had the opportunity to read all; I read all but we can come back at the next hearing and if we agree that we still want to hear Grenville Phillips, do not mind he has written, we are just using him as an example, we can hear him.

Asides.

Mr. CHAIRMAN: That seems to be the consensus, because we are not agreeing on anybody else. The Minister, Minister Marsha Caddle; wants the opportunity to come before the Committee and that is her privilege under the rules to ask to come and also Sir David Simmons would like to come back because when you read many of these submissions, honestly, a lot of them are criticising what he said and in fact, asking him to respond. I think it is only fair that Sir David Simmons be given a time to come back. He and Minister Caddle can come on the same afternoon.

Senator R. O WALTERS: How much time will each of them have to respond?

Mr. CHAIRMAN: We are going to have to set that but an afternoon with just the two (2) of them and be finished off. In other words, can we meet again? I had asked if all day Monday, but I recognise we have busy professionals in here but when I was on the Medicinal Marijuana Committee, we met all days. Is it possible to meet on Monday from 9:30? Leader of the Opposition, how is your schedule for Monday next week?

Asides.

Mr. CHAIRMAN: And your schedule?

Mr. P. R. PHILLIPS: What day is that?

Mr. CHAIRMAN: Monday, next week. Tomorrow is Parliament. Wednesday, Thursday and Friday, as I understand it, is the Parliamentary Reform Commission. They are trying to finish their report; having gotten an extension or two (2) already. Monday, 10 o'clock then? Monday, 13 May, 2024? Okay. The five (5) orals in the morning. We break for lunch on Parliament; we will hear that tomorrow. In the afternoon, Minister Caddle and Sir David Simmons.

Mr. P. R. PHILLIPS: Caddle?

Mr. CHAIRMAN: She has the right under the rules to come and she has asked to come.

Mr. CLERK: Mr. Chairman, let me just be clear because you had in your email that she is proposing at 2:00 p.m.

Mr. CHAIRMAN: Right. In other words, after lunch.

Mr. CLERK: Okay. We will break at 1:00 p.m. for the lunch session.

Mr. CHAIRMAN: We should be able to do five (5) in the three (3) hours between 10:00 a.m. and 1:00 p.m.

Mr. CLERK: Well, we control the time. We tell persons 10 minutes and then limit the questions within the three (3) hours.

Mr. CHAIRMAN: Even if when we work it out, we tell her 2:30 p.m. to give us some space?

SENATOR G. P. B. NICHOLLS: Two o'clock is good, Mr. Chairman because we have her and Sir David Simmons. It would get a little counter-productive if we were here all day into the evening.

Mr. CHAIRMAN: Right. Exactly. The Senate is not meeting before Monday next week. If when Members deliberate; read the papers; Monday afternoon you come and there is consensus that we really need to hear Maureen Holder or Cammie Holder, in any event we are going to have to ask the Senate for an extension to write the report. Monday is within the 90 days set by the Senate. Unless Members, there is consensus on hearing any of these written submission people, we could wrap within the 90-day period and just ask the Senate then for additional time to write the report.

We agree? Honourable Leader of the Opposition? Reasonable?

Mr. R. A. THORNE: Yes.

Mr. CHAIRMAN: Good. Alright. Just make sure we read every one that is received. So, Monday at 10:00 a.m. Mr. Clerk, we would set out times for everybody. The five (5) between 10:00 a.m. and 12:30 p.m. to come? Alright. Break for lunch. Invite Minister Caddle. Who should go first? Minister Caddle or Sir David Simmons, you would think?

SENATOR G. P. B. NICHOLLS: Sir David Simmons.

Mr. CHAIRMAN: Sir David Simmons will be first and then, Minister Caddle to wrap up. Alright. Obviously, then to write the report, give us guidance Mr. Clerk on. No, that is just a time I set for her.

Mr. CLERK: No, I was just wondering if she had.

Mr. CHAIRMAN: I have no idea. I do not know. I set that time for her. I told her that is when I will propose that she comes. Tomorrow, I could ask her. If the feeling is she should go last, I would tell her and see if that is okay. Alright. The last, Other Business, I have realised Members that the Police Service Commission sent in a submission last week after our deadline. Do we still accept it? In other words, I got it and thought all of you were copied in, unless Senator Nicholls. I realise, you were not getting some emails.

SENATOR G. P. B. NICHOLLS: No. I was getting my emails. I read the submission from the police.

Mr. CHAIRMAN: Even though it was sent in after the time….

SENATOR G. P. B. NICHOLLS: Mr. Chairman, it was from the Commissioner not the Police Service Commission.

Mr. CHAIRMAN: Sorry. I said Service Commission? The Barbados Police Service. Sorry. From the Police Force then. Right. Whether it was saying something or not, do we still note it in the report? Do we agree to still include it, even though it came in after time? That is all I need to know.

SENATOR G. P. B. NICHOLLS: Mr. Chairman, it has already been circulated, so….

Mr. CHAIRMAN: So, we include it. Okay. Motion for adjournment until Monday, 13 May, 2024 at 10:00 a.m.

ADJOURNMENT

On the motion of Senator G. P. B NICHOLLS seconded by Mr. P.R. PHILLIPS, Mr. CHAIRMAN adjourned the Joint Select Standing Committee meeting until Monday, May 13, 2024 at 10:00 a.m. in the Senate Chamber.

4th MEETING
JOINT SELECT COMMITTEE (STANDING)
ON
GOVERNANCE AND POLICY MATTERS
ON THE
CYBERCRIME BILL, 2024
AND THE
MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024

Monday May 13th, 2024

PRESENT:

Mr. Edmund G. HINKSON, S.C., MP, LL.B. (Hons.), L.E.C., LL.M. **(Chairman)**
Dr. Romel O. SPRINGER, J.P., MP., PH.D., **(Deputy Chairman)**
Mr. Peter R. PHILLIPS, MP
Mr. Ralph A. THORNE, K.C., LL.B., L.E.C., Dip. Theology
Senator The Hon. Lindell E. NURSE, F.C.A, F.C.C.A., R.C.S. (ENT)
Senator Gregory P. B. NICHOLLS, B.Sc. (Hons.), LL.B. (Hons.), LL.M., MCIArb.
Senator Ryan O. WALTERS, M.B.A.

ALSO IN ATTENDANCE:
Mr. Pedro EASTMOND, (Clerk of Parliament)
Ms. BEVERLEY GIBBONS, (Deputy Clerk of Parliament)
Miss Suzanne HAMBLIN, (Journal Department of Parliament)
Ms. Rhea DRAKES, (Office of the Chief Parliamentary Counsel)

PRESENTERS:

Janine Butcher
Victor Lewis
Heather Cole
David Weekes
Timon Howard
Hon. Miss. M. K-A. CADDLE B. A., M.Sc

Call to Order
The Chairman called the meeting to order at 10:45 a.m.

Mr. CHAIRMAN: Good morning, everyone. Welcome and trust that we all had an enjoyable weekend. It was an opportunity for us to honour our mothers, if they are still with us and you know, we had some cricket last night as well.

We are going to defer the minutes of the third meeting and consequentially will defer Matters Arising. We are into oral presentations by Janine Butcher; I understand she is on Zoom? Victor Lewis is here? He is downstairs, right. I understand we have not gotten hold of, at least Miss Roslyn Corbin has not responded? Is that correct? So let us link up to hear Ms. Janine Butcher. Remember, they each have 10 minutes maximum to present and then any member can question them. We have allocated, generally speaking, a half hour for each person.

Good morning, Miss Butcher, can you hear us?

Miss Janine BUTCHER: Good morning. Yes, please, can you hear me as well?

Mr. CHAIRMAN: Good morning, Madam. Welcome to the Standing Committee of Parliament on Governance and Policy, to discuss the Cybercrime Bill and the Mutual Assistance in Criminal Matters (Amendment) Bill. You had indicated that you wished to give oral testimony before us.

We will permit you to do so for 10 minutes and then any Committee Member can question you. We have four (4) Committee Members here today: Leader of the Opposition, Honourable

Ralph Thorne, King's Counsel (KC) is here; we have the Honourable Dr. Romel Springer, Member of Parliament (MP), Parliamentary Secretary; we have the Honourable Mr. Peter Phillips, MP, who is Chairman of Committees of Parliament and myself chairing, Edmund Hinkson, Member of Parliament, Senior Counsel (SC).

Apologies for a slightly late start and for keeping you waiting. State your name for the records, Madam.

Miss Janine BUTCHER: Honourable Members of both Houses; Members of the Joint Select Committee; Mr. Chairman; ladies and gentlemen, good morning, my name is Janine Butcher.

Mr. CHAIRMAN: You are giving your testimony by Zoom**,** so I am assuming you are not in Barbados?

Miss Janine BUTCHER: Not currently.

Mr. CHAIRMAN: Okay, so where are you residing?

Miss Janine BUTCHER: I am not there now but I live in Barbados.

Mr. CHAIRMAN: Okay and for the record, what is your occupation?

Miss Janine BUTCHER: I am a Customer Service Representative.

Mr. CHAIRMAN: Okay, Ms. Butcher, the floor is yours.

Miss Janine BUTCHER: Before beginning, I would like to state that I spoke to young persons about their views on this Bill and incorporated what they said into my presentation. I am no expert but just someone who utilises a social media platform.

Today we gather here to address an issue that strikes at the very heart of the future. Challenges facing globalisation in this technological world, is analysis of the establishment of Cybercrime Bill 2024, which will be the future cornerstone of how we interact and communicate among each other; especially among the youth that love social media.

This Cyber Crime Bill 2024, encompasses a comprehensive legal framework to address various offences related to cyber activities, providing authorities with the tools to investigate, prosecute and deter cybercrime. I am in agreement with many things here and that it is necessary to have this open discussion that if changes are needed for this Bill, they should be considered and finally, that cybercrime is real and active in our daily lives.

Many countries in the Caribbean have introduced this type of Bill in which they had to go back to the drawing board to change, shift and at some point, delete the entire aspects, that breach our human rights laws, that we in the region, have signed onto.

For instance, in Trinidad, when it was first introduced in May 2015, the Cybercrime Bill was heavily criticised by media and human rights organisations, including the Centre for Law and Democracy, for vague and overboard content offences which would have prohibited a range of innocuous, normal or even beneficial online activity. Despite some minor revisions, the current versions of the Cybercrime Bill (in Trinidad) still suffers from these problems in its new one (1) passed again in 2017.

Also in Jamaica, the Cybercrimes Act of 2010, 2015 and 2021 is undergoing review and amendments as the need increases for integrating laws concerning cybercrimes. On the face of it, this sounds simple enough and is a Bill most citizens would support to protect themselves from potential harm, where these types of laws are not in place. There is a delicate balance to ensuring, retaining and encouraging technology students and professionals to innovate and experiment. As a result, I am proud of our nation for taking our time, doing our research and talking to the larger community, to figure out why and what aspects of this Bill hinder Barbados' development on how we balance our rights versus the crime.

Today, I will tackle two (2) important areas of the Cybercrime Bill 2024, including police force law enforcement. While this legislation aims to empower law enforcement officials in combating cybercrime, it must be carefully crafted to respect individuals' rights to controlled access to their information. Procedural safeguards,

judicial oversight and transparency are key elements in achieving this balance.

Potential for abuse: There might be concerns about the potential for abuse of the legislation for political or personal reasons. The expansive powers given to law enforcement agencies should be carefully balanced to prevent misuse. Indeed, the potential for abuse is a critical consideration when assessing legislation, especially when it grants expansive powers to law enforcement agencies.

Here is an analysis of the potential for abuse in the context of discussed legislation and some recommendations to be put in place for Parliament to consider.

Political interference: Given the broad scope of the legislation, there may be concerns that it could be used to stifle political dissent. Safeguards in the law should be in place to prevent the legislation from being misused to target individuals expressing legitimate political concerns or opinions, thus upholding the principles of free speech.

Selective enforcement: The legislation must be applied uniformly and without discrimination. There should be safeguards to prevent selective enforcement based on political affiliations, personal vendettas or other non-criminal motivations. Hopefully, everything goes being unbiased.

Whistleblower protections:
Whistleblowers play a crucial role in exposing wrongdoing. The legislation should include provisions to protect whistleblowers who may be disclosing information in the public interest. This prevents the legislation from being used against individuals seeking to expose corruption or misconduct.

Oversight mechanisms: Establishing independent oversight bodies separate from law enforcement agencies can help mitigate the risk of abuse. These bodies can review the application of the legislation, investigate complaints and ensure that powers are exercised within the bounds of the law.

Clear legal standards: Offences outlined in the legislation should be clearly defined to prevent arbitrary or subjective interpretation. Clear legal standards help ensure that law enforcement actions are based on objective criteria; reducing the potential for abuse.

Judicial review: Providing avenues for judicial review of law enforcement actions is essential. This allows individuals to challenge the legality of searches; seizures or other actions, ensuring that the judiciary acts as a potential on abuse.

Protections of minority rights: Safeguards should be in place to protect the rights of minority groups. The legislation should not be used disproportionately against specific communities, ensuring that the rule of law is applied impartially.

Transparency and accountability: Regular reporting to the application of legislation, including the number of nature of cases, contributes to transparency. Public awareness of law enforcement activities helps to deter abuse and hold authorities accountable.

International human rights standards: Ensuring that the legislation aligns with our human rights standards helps establish a framework that respects fundamental rights and freedoms. Compliance with established norms reduce the risk of misuse. In conclusion, safeguards such as independent oversight, clear legal standards and protection for whistleblowers are essential to mitigate the potential for abuse associated with the legislation, that grants extensive powers to law enforcement agencies. Let us reflect on these vital questions in terms of the police force, law enforcement and engagement in this Bill.

Thank you for allowing me to make this contribution. I do have a few questions in closing. They are as follows:

- How much would it cost the police force to establish this new department to combat crime?

- How much will it cost the country's taxpayers, in terms of police manpower?

- What will the cost of implementing resources and equipment be?

- Is the police force willing to participate in this Bill?

- Can we manage our national crime versus our online crime?

Those are my questions. Thank you.

Mr. CHAIRMAN: Thank you, Ms. Butcher. I must say that two (2) other Members of the Committee have just joined us. Welcome Senator Gregory Nicholls and Senator the Honorable Lindell Nurse. Now, as regards to your questions, Ms. Butcher, this is a Committee of Parliament. In other words, this is a Standing Committee of the legislature. Under our system of Government, as I am sure you know, we have separate arms of Government that make up, you know, our governance structure.

The questions that you have posed are not within the ambit of this Committee or legislature. I am not saying they are not very relevant or pertinent questions, Madam. How much it will cost the police to set up, you know, a cybercrime department to investigate alleged breaches of the legislation when enacted by Parliament? It is a pertinent question but that is not within the ambit. You will have to carry your questions somewhere else, Madam, you could appreciate. Alright.

You spoke in terms of the oversight. Someone, at least one (1) person I think, who sent in a written submission spoke about what they perceived as a need for an oversight body as well. How you perceive such an oversight body would work?

Ms. Janine BUTCHER: Sorry. Can you hear me now?

Mr. CHAIRMAN: Sorry. Did you hear the question?

Ms. Janine BUTCHER: Yes, please. Sorry about that. Right. So, your question was how an oversight body will work from my point of view?

Mr. CHAIRMAN: Yes, Madam.

Ms. Janine BUTCHER: As I would have stated, in terms of establishing independent oversight bodies, separate from the law enforcement agencies itself.

Mr. CHAIRMAN: Right but would that not just add to the bureaucracy of the situation?

Ms. Janine BUTCHER: I do not understand the question?

Mr. CHAIRMAN: No, you are now talking about another body separate from law enforcement. I mean, you also have the judiciary that is there; that once someone is charged will have to hear the case and make a judgement on the matter. So, is that not sufficient oversight and bureaucracy? Why do you want to add another layer of bureaucracy to a situation?

Ms. Janine BUTCHER: In terms of being unbiased and the manpower which I would have stated as well. So, the body that you are speaking of has efficient manpower to oversee the Cybercrime Bill alone, as well as the other crimes that we have in Barbados as well?

Mr. CHAIRMAN: No but like I said, we are a legislative body. I am sure that once the Bill is passed and enacted, those with responsibility over the police department would adjust and operationalise the matter. Alright. As I said, that is not for us to be concerned with here. Okay.

Ms. Janine BUTCHER: I understand.

Mr. CHAIRMAN: Any Members would wish to engage, Ms. Butcher? Okay, Ms. Butcher. We thank you. Your testimony is on record and will be part of the report of this Committee. We thank you for your engagement with us and for your keenness to be part of this process. Okay.

Ms. Janine BUTCHER: Thank you for having me.

Mr. CHAIRMAN: Okay. Good Morning.

Ms. Janine BUTCHER: Good Morning.

Mr. CHAIRMAN: Mr. Lewis, your turn to engage us, Sir and to have the floor for 10 minutes. You can come and sit down here, Sir. Good Morning. Mr. Lewis, for the record, you can state your name and your occupation. Okay, you have the microphone. Press it on, Sir.

Mr. Victor LEWIS: My name is Victor Lewis and what is the other bit of information? I am retired.

Mr. CHAIRMAN: You have 10 minutes for the oral presentation and that as you heard, you have 10 minutes of oral presentation and then any Member can engage you on anything that you have said.

Mr. Victor LEWIS: That is fine and you can start anytime? Okay again, good morning to everyone. I am of the view that checks and balances are important for the development of our country. The ability to take any computer device; catch information and publish it is healthy even amongst pain in the interest of development of Barbados. This attitude in the formulation of this Bill seeks to criminalise free speech and in my view, this is not in the best interest of the development of our country.

Could we imagine that **Darnella Frazier,** a 17-year old teenager; standing on the streets of the United States of America (USA); having a fear of imprisonment or fine? We would not have heard that cry, *"I cannot breathe!"* They are many **Darnella Fraziers** in our country. Let us not drive fear into our people but let us create an environment, where our people can freely ventilate their feelings.

I want to turn to the document. The Cybercrime Bill, page one (1) and this is what I have downloaded, so I am of the view that downloading it from the internet, that I have a legitimate document. It starts off with the heading "Objects and Reasons". I am of the view that that particular statement is very questionable. I am of the view that this document should start off with objectives and clearly this document in the first page should be separated; not reasons and objects. I do not know what you mean by objects. It ought to be objectives.

Mr. CHAIRMAN: Mr. Lewis, I am trying to follow you. Where are you looking?

Mr. Victor LEWIS: I am looking at the document that I downloaded and it starts off with, "This Bill will provide for" and at the heading it has "Objects and Reasons".

Mr. CHAIRMAN: Sir, the Bill itself does not have that and I will give you back your time, Sir. You can appreciate that there is, okay; "Objects and Reasons". That is drafting. Okay. Hold on. That is how the drafters; Legislative Drafting is an art.

That is a course that all law students take and then they are people who specialize in legislative drafting and that is how, in Barbados, all Bills that come before Parliament have at the front, "Objects and Reasons" so that is a legal technicality, drafting technicality and I do not know if you are an Attorney-at-Law but all Attorneys-at-Law and they are right now four (4) in here, including a representative of the Chief Parliamentary Counsel (CPC) who would explain to you as to how it is done in Barbados.

Ms. Rhea DRAKES: Thank you very much, Mr. Chairman. Just to clarify that the "Objects and Reasons"; this is more or less standard in all pieces of legislation; all Bills. The same way you would have an arrangement of sections or parts, so this is a consistent drafting style and this is seen universally. Thank You**.**

Mr. Victor LEWIS: I am of the view that as a heading drives the content. I am of the view that as a heading informs the content and if you would just give me some time let me scroll back to that document because I heard on the radio, Ms. Caddle, who spoke on this document and what was said to me was confusing because when we look at Item B in that first page. It says, *"The protection of legitimate interest in the use and development of information technologies".* But, when Ms. Caddle spoke on the radio she said, *"Protects legitimate interests and development".* Those two (2) statements are clearly ambiguous.

They do not mean the same thing so I am saying that when we have this document that is classified as the Cybercrime Bill, it ought then to drive content so that people are not misguided; so when we read, "Objects and Reasons"; these objects and reasons must be clearly defined, not only the objectives but also those enablers that will drive the objectives. Those tools that will be mobilized in order to achieve these objectives.

I want to go onto 19(1):

"A person who intentionally or recklessly uses a computer system to publish, broadcast or transmit computer data that intimidates a person."

Intimidates by this document is said to mean a reasonable person. A reasonable person is one who is acting within the law then my question is if a reasonable person is deemed to be such a person who is acting within the law, then manipulation of the law gives an individual the opportunity to make a reasonable person unreasonable and an unreasonable reasonable; just by manipulation of the law. If then we want to consider what is happened in our country of late; when we change Town and Country Planning to Planning and Development where once we had, a head or Chief Town Planner but now we have the Prime Minister of Barbados in charge of Planning and Development; where that individual can manipulate the laws of Barbados so when anyone has been given the opportunity to manipulate the law of our country; that person then in the manipulation of those laws, can change a reasonable person into an unreasonable one.

Mr. CHAIRMAN: Okay, Mr. Lewis, for the records I have to correct you, Sir. I cannot let something that is absolutely erroneous, go on the records of Parliamentary Standing Committee.

First thing, Sir, the Prime Minister of Barbados and we are talking about the office, not the individual; cannot manipulate any department that oversees Town Planning. The Minister in charge of planning right now is not the Prime Minister but Senior Minister William Duguid.

Historically, since Independence, virtually every person who has held the office of Prime Minister, has been Minister in charge of planning except for a short period of time when now Ambassador, Senator Elizabeth Thompson was Minister of Planning under the Owen Arthur Administration for, I think it was for two (2) years and now, with Senior Minister Duguid being Minister of Planning since last year, April.

Under our system, a Minister of government has ultimate responsibility over any department that they have cabinet responsibility over but if you were to read, Sir, legislation that was passed in 2020 or 2019, you will see the checks and balances in terms of planning decisions. There is also a tribunal and there is an appeal process, all of that, Sir, without a Minister becoming involved.

I cannot let what you said erroneously go on the record of Parliament without correcting you, Sir and there is no difference, now, to the situation than it was previously in terms of ministerial ultimate responsibility, in terms of planning.

Mr. Victor LEWIS: Is that it, Sir? May I continue? Thank you very much. Now, when I consider the pledge of our country which everyone must uphold and defend and by my living to do credit to my nation, wherever I go. When I go to St. Michael, for example and I examine what is happening on the train track; I, as a Barbadian, realise that the application of the laws in that area, appear to be different to the application of the laws in St. Joseph, so I am confused.

Nevertheless, let me go to my final item and this is 23 (1) in the document: *"…reasonable grounds…that a crime is about to be committed".* How ambiguous that statement can be? *"…reasonable grounds…that a crime is about to be committed"*. I am not only retired, I am a retired educator and a retired police officer. So how am I to interpret that "*a crime is about to be committed?"*

On 24 April, 2023, at 11:57 p.m, my cameras captured a police vehicle by my house. I live in a cul-de-sac; at the end of the cul-de-sac. You have to drive off the paved road to get to my house. Around that same time, I made several videos and I do not know if a police officer felt emboldened by this document, that they have the right to turn up at my house, with a view that a crime was about to be committed. This document …

Mr. CHAIRMAN: Mr. Lewis, your time is up. Thank you very much, Sir. Please, one (1) sentence to wrap up.

Mr. Victor LEWIS: In Daniel, Chapter 12, verse one (1): *"There is coming a time of trouble such as never was*". That time is coming where AI will be dwarfed. How will a Cybercrime Bill address a situation in that period of time? Truth must not only be seen to be absolute, not qualified, absolute. Let us depend on the word of God to drive this Cybercrime Bill.

Thank you very much.

Mr CHAIRMAN: Thank you, Mr. Lewis. Any Members wish to question or engage Mr. Lewis on anything he said?

Dr. R. O. SPRINGER: I was just going to comment on what Mr. Lewis would have said last about a crime about to take place. I think those were the words used which were used? Yes, words within the Bill.

And I am going to discuss with you and answer the question I asked Mr. Stuart at the end of his presentation last week.

Mr. Victor LEWIS: Your name, Sir?

Dr. R. O. SPRINGER: My name is Romel Springer. Now, are you aware of cyber grooming? The concept of using social media; using the Internet; using WhatsApp; what have you, to lure young girls; young boys; whatever you are into. Lure them into locations for the purpose of engaging in some kind of prurient activity with them.

Now, at some point, I mean, at some point the crime is not yet committed but you can see that the buildup is there. You can see the person is making plans; they are talking to the young child; they are telling them how they look; they are giving them compliments; you know. Then, they are arranging to meet them; they want to see them and they miss them and all these things they are saying; all of this with a view that at some point to get that young child, young boy or girl, to meet them in some place in the physical space, so they can engage in a prurient activity with that person.

Is that not a crime about to be committed? Is that not something that police should be able to get a handle on and make an arrest before it even happens? Or should we wait until the child is raped or engaged in some sexual activity for police interaction and a report is made? Is that what you are suggesting? That the police should not have that flexibility or the power to arrest in a situation like that before it occurs?

Mr. Victor LEWIS: I spent some thirty-something years in teaching. I was a year-head. I was in charge of many students. I am aware that the whole idea of this aspect of pornography and computer crime became part of the laws of Barbados in 2005. This is 2024, 19 years after; we are well au fait that this dimension has been addressed by the Government of Barbados, to protect the people of Barbados.

I would have a big difficulty, when my children cannot go into a river and play. That is something now that I must seek to protect. We have already put systems in place to protect our children against cybercrime when it comes to pornography; that is old news, Mr. Springer.

Let me get to a point now where we have rivers in Barbados that our children can freely go and play. When we have developers coming to our country to prevent them from enjoying the rivers. At the Alleyne School, we had a department for the whole interest of the community, dealing with the environment. So we had an environmental group where students could freely go over to Long Pond and enjoy themselves freely or go over to Joe's River and enjoy themselves…

Mr. CHAIRMAN: But Mr. Lewis, what does that have to do with the Cybercrime Bill? No, Sir. Refine your comments and your responses to the Cybercrime Bill, Sir. This is not a forum for you to vent on what you see as the wrongs of Barbados society. Deal with the Cybercrime Bill, please or on Mutual Assistance...

Mr. Victor LEWIS: Well, let me say to the gentleman, that is old. We have dealt with that since 2005.

Dr. R. O. SPRINGER: Sir, Sir, with all due respect, I am not speaking about pornography. I said nothing about pornography. I am talking about cyber-grooming; I am talking about luring young boys and girls, by way of social media or Internet or WhatsApp. That is what I was referring to.

Mr. Victor LEWIS: When you talk about luring. When you talk about luring, Sir, it means that you are using social media; internet and Facebook to pretend that you are nice, 19-year-old boy; when you are 67-something years old. That is luring. That is using social media. That is using computer systems that has been dealt with since 2005. That is all I am trying to say.

Dr. R. O. SPRINGER: What I am saying to you and I do not think you understood exactly what I was getting at. The idea of systems or legislation in place to treat to these things before they get to the physical stage, before it even happens…

Mr. Victor LEWIS: But, I am saying that that legislation was in place since 2005.

Dr. R. O. SPRINGER: Before it even happens….

Mr. Victor LEWIS: But since 2005, Sir, that has been there. That is nothing new. What we are dealing now with new is other things that affect our children; that affect the children of our schools; that affect children at the Alleyne school; that affects children at synergies of primary. Those are the things that we have got to deal with now. Those tools are already in place to address that long time ago.

Dr. R. O. SPRINGER: Where in that 2005-legislation speaks to cyber-grooming?

Mr. Victor LEWIS: Well, you need to know.

Dr. R. O. SPRINGER: You are making the claim. You are making the claim that it is there. You are making the claim in response to what you said which is my question that simply asks, why should not the law have the ability to intercept these things before they even occur?

Mr. Victor LEWIS: Sir, you could go and read the Computer Misuse Act; it is there. It is clear. We do not have to deliberate on that in the 10 minutes that I have here. We can deal with it in another forum but certainly it is there in the Computer Misuse Act; that is not rocket science.

Dr. R. O. SPRINGER: Are you not going to answer my question? Thank you very much.

Mr. Victor LEWIS: Thank you.

Mr. CHAIRMAN: Any other Members wish to engage, Mr. Forde? Just one…. Mr. Lewis, sorry. Just one (1) more query I am going to ask you. You started by saying, Sir, you made a very fiery statement that this Bill will curtail free speech, you said exactly. Please point me to the section in the Bill which will "criminalise", that is the word you use, free speech. Point the section out.

Mr. Victor LEWIS: You would appreciate, Sir, that, you know there are certain conditions on which I speak. But, I….

Mr. CHAIRMAN: What conditions, Sir?

Mr. Victor LEWIS: You know, those things that are before the court.

Mr. CHAIRMAN: Sorry?

Mr. Victor LEWIS: Those things that are before the court?

Mr. CHAIRMAN: No, Sir. I am absolutely not understanding you. You made a very blatant, fiery statement and I would like you to assist this Committee by pointing to the provision in the Bill which supports your statement that the Bill will criminalise free speech Straightforward, Sir.

Mr. Victor LEWIS: Yeah, I know it is very straightforward. No problem. So let us go to….

Mr. CHAIRMAN: I thought it would be at your fingertips. No, No, I did not think that you would have to now go looking for it.

Mr. Victor LEWIS: I got to a roll back my computer. I do not have that printed out. Why should I print that out? Let me just roll my computer. Give me a few seconds, Sir. Let me just roll. I think it is 19(1). Let me just roll. You know, I said I would have made several videos over the course of time and after making those videos, I received several threats not from Barbados, you know, from outside of Barbados; from developers. Threats to the extent that I would capture information and I do not want to be specific but of course, I told you, I am from St. Joseph. I enjoy St. Joseph and other places.

Mr. CHAIRMAN: Sir, I asked you a specific question. I did not ask you where you come from and all of that.

Mr. Victor LEWIS: Fair enough, Sir. Let me just continue to roll. Clause 19(1)(a). Well, let me just deal with Clause 19 (1). It states, *"A person who intentionally or recklessly"*. Recklessly is a very ambiguous and derogatory

statement. It continues, "A person who intends…"

Mr. CHAIRMAN: No, you do not have to read it, Sir. We know it. Clause 19 (1) (a).

Mr. Victor LEWIS: I took my cell phone and captured information as to what was happening at Joe's River in St. Joseph. I broadcasted it and then, I received threats from the developer.

Mr. CHAIRMAN: No, Sir. Sir, what happenned with you and the developer; that is irrelevant to this Committee. You are saying that Clause 19(1)(a) criminalises free speech in Barbados. You believe that an individual should be allowed to intimidate a person; to threaten violence on them; to threaten to kill them; to damage their property; to damage the property of their family intentionally, Sir. In other words, they have the mental capacity to do that or recklessly, by way of a computer and should be able to get away with it.

Mr. Victor LEWIS: I do not know what you mean by kill.

Mr. CHAIRMAN: Well, kill is a normal word. "I gine kill you today".

Mr. Victor LEWIS: Kill means to take a life, so I am not going to use that word.

You feel that someone should be able to use the computer to tell someone, "I g'ine kill you today. I gine kill your mother today." That is okay with you? Yes or no, Sir. That does not need any….

Mr. Victor LEWIS: I cannot answer yes or no.

Mr. CHAIRMAN: Okay, Sir. Alright, that is no problem. That is no problem. You cannot answer.

Mr. Victor LEWIS: Not yes or no? I can answer but I cannot answer yes or no.

Mr. CHAIRMAN: It is a simple no.

Mr. Victor LEWIS: No. That is not simple. When you ask of question, you must give individuals the space in order to give the answer they want to give.

Mr. CHAIRMAN: Alright, Sir.

Mr. Victor LEWIS: I will not be forced into yes or no. We have passed that stage in our development.

Mr. CHAIRMAN: What answer you want to give?

Mr. Victor LEWIS: Not that I want to give. If I am given the floor then to respond, I will respond but not yes or no.

Mr. CHAIRMAN: Let me hear your response then, Sir, to that question.

Mr. Victor LEWIS: Could you repeat your question, Sir?

Mr. CHAIRMAN: I thought I repeated it already. That you said, Section 19(1)(a) criminalises free speech and all I am asking you, is if you believe that somebody should be allowed to tell Victor Lewis, *"I am going to kill you today. I am going to kill your mother. I am going to burn down your house; kill your daughter and get away with it."* That should not be subject to criminal law?

Mr. Victor LEWIS: I cannot deal with extreme examples.

Mr. CHAIRMAN: No, Sir. No. Okay. So, you have answered the question, Sir.

Mr. Victor LEWIS: Thank you very much.

Mr. CHAIRMAN: Okay, Sir. So, we thank you for your….

Dr. R. O. SPRINGER: I just want to clear one (1) thing for the record because he quoted the Computer Misuse Act. I want to just state for the record that there are no provisions in that Act for cyber-grooming. I do not know where you read it. I read the entire Act. It is not there.

Mr. Victor LEWIS: It is not there?

Dr. R. O. SPRINGER: No.

Mr. Victor LEWIS: So, in specific terms?

Dr. R. O. SPRINGER: Well, we are dealing with specifics.

Mr. CHAIRMAN: There are periods, Sir, whether in specific terms or not, it is not there. So, we thank you, Sir, for your evidence today. Good Morning.

Ms. Rhea DRAKES: Mr. Chairman.

Mr. CHAIRMAN: Yes, Madam.

Ms. Rhea DRAKES: I just wanted to add something with your permission.

Mr. CHAIRMAN: Sure.

Ms. Rhea DRAKES: References made to the line or the provision in the legislation about a crime being committed or is about to be committed, that is currently the law, Section 23 of the Computer Misuse Act. The other thing that Dr. Springer would have raised in relation to giving police the investigative tools or the ability to intercept any possible threats. So you gave an example about child grooming but also the case,

for example, where a hacker may say, "Well, we are going to give the government X period otherwise, we are going to attack all of its critical information systems." In a case like that the police would rightly believe that a crime is about to be committed. Thank you.

Mr. CHAIRMAN: Thank You, Madam. Okay. Good, Sir. Next person is; welcome, Senator Walters. Good morning.

Asides.

Mr. CHAIRMAN: Ready? Good morning Ms. Cole, can you hear me? Ms. Cole? Why is she not responding? Okay. Good morning, Ms. Cole. Can you hear me? Ms. Cole, is your audio on? She has disappeared now. I wonder what happened here. Her time was 11:45 so you want to give her.

Ms. Heather COLE: Hello. Can you hear me?

Mr. CHAIRMAN: Hello, Ms. Cole. You are hearing us now. Yes, you have come on earlier than we said you would, so we thank you for that. Welcome to the hearing on the Cybercrime Bill and the Mutual Assistance in Criminal Matters Amendment Bill before the Governance and Policy Committee of Parliament, Standing Committee. We have here five (5) Members of the Committee, in fact, six (6) Members of the Committee including The Honorable Leader of the Opposition and Senator Ryan Walters; The Honourable Lindell Nurse sorry, Senator; Mr. Peter Philips, Member of Parliament; Senator Gregory Nicholls and myself, Edmund Hinkson, Member of Parliament.

We are going to permit you 10 minutes, Madam, to speak on either of these two (2) Bills or both of them. Your comments on them; whatever you wish to say on them, that is of relevance and then Members would be given the opportunity to engage you on anything you have said. Your name for the records.

Ms. Heather COLE: Heather Cole.

Mr. CHAIRMAN: Where are you right now? Are you in Barbados or overseas?

Ms. Heather COLE: In New York City.

Mr. CHAIRMAN: So you live in New York?

Ms. Heather COLE: Correct.

Mr. CHAIRMAN: Okay Madam. What is your occupation for the records?

Ms. Heather COLE: I am a Budget Analysis.

Mr. CHAIRMAN: Okay, so you have 10 minutes.

Ms. Heather COLE: Alright and I will read my submission and it is in relation to the Cybercrime Bill. My primary cause for concern or one (1) of them and I have three (3). Last Monday, 06 May, 2024, I listened to Mr. Steven Williams in his presentation to this Committee and when he was being questioned after his presentation, he spoke stating that he hoped.

Mr. CHAIRMAN: Okay, Ms. Cole just hold a minute because it is coming through very loud. Okay, Ms. Cole. It is coming through very loud, so speak again.

Ms. Heather COLE: Alright, well let me try it again.

Mr. CHAIRMAN: Okay, so we are good now. We are good. That is good volume.

Ms. Heather COLE: Great. As I listened to Mr. Williams last Monday, when he was being questioned he spoke that he hoped that the Great Firewall of China was not the way that the police intended to go and Mr. Williams was the government's consultant on this project and he went to China to get first-hand information; so at that point I made a note that he has referenced the great Fire wall of China and later, I went back to the Bill and I saw no mention of surveillance and detention within the Bill.

In China, surveillance and detention go hand in hand; one (1) does not happen without the other and then I looked at Section 23 (3) as well as Sections 24 and 25 and I am referring to the Cybercrime Bill and neither of these sections stated what happens to any person after the search or prior to an appearance in court. Let me go on and it appears that the consultant is unaware of the outcome of his project, even though he was the technocrat and would have had the best recommendations to give to the Government.

At this point in time, I know that the word "hope" is a bad word in Barbados, so I have no hope in Mr. Williams' "hope" because right now in Barbados "hope" is referenced to me in things like wastage; misuse of funds and corruption; *et cetera*. Again, having heard the consultant use the Great Firewall of China, I explored it for what it is, a heavily surveillanced police society where nothing can happen except the police are aware. All of the internet traffic, both in and out, must pass through the police.

China is also a society where they use an Identification Card (ID) that is similar to the Trident ID and it is a method of surveillance; control. Surveillance and detention centres go hand in hand in China, so based on the revelation of the consultant, I now wonder if the Government of Barbados is planning to build or has already built a mass detention centre in Barbados.

If this is true, this Bill will become a warrant for torture and death in detention for the sons and daughters of Barbados. Mr. Williams' revelation, in my opinion, was like a missing piece of the puzzle. I now wonder if Barbados is about to become a police State and I am assured that all Barbadians would want to join me to insist that the Government of Barbados address this before it proceeds because I do not think that we should be welcoming Chinese slavery in Barbados.

That is my first concern. The next one (1) is the Constitution. We have awaited the new Constitution for quite some time and I wonder now, if the new Cybercrime Bill was being put in place, to be followed by the new Constitution or if the Constitution was waiting for the Trident ID as well as the Cybercrime Bill to be in place then for the Government to present it.

If that is the case, I wonder now how this will affect the freedoms of expression that are currently available in Barbados? Technically in this area there are too many unknowns and I also wonder, for example, if it could be unconstitutional to protest with marches. The next piece of my presentation references me personally. I was a victim of cybercrime that was committed against me in 2018.

I came to Barbados and I gave a statement to the police and on the morning of the second day, I went back to the police station again and upon leaving the room where I was being interrogated, I overheard the Station Sergeant tell someone on the telephone, "de woman here!". As I passed his desk and he realised that I was passing, he lowered his voice and he quickly ended his conversation, so I had no idea with whom he was speaking.

The police took my phone and it was not ready by the time I was ready to leave the island the next week; so I went back for it. I sent it back to Barbados the following month and it was to be collected from the Worthing Police Station but that did not happen. I returned to the island the next year and went to Worthing Police Station, where another officer met me and I finally collected the phone. I kept in contact with the police for updates regarding the case but nothing was forthcoming.

My brother called continuously and if the Sergeant answered the phone or whoever transferred the phone to the Sergeant, they would say an arrest was imminent or tell him something

to get him off the phone. Most times the phone rang off the hook.

Years went by. I wrote to the Prime Minister, got no response. I wrote to the Consul General in New York, got no response and I wrote to the Director of Public Prosecution (DPP) as well as to the Commissioner of Police but got no response.

I learned that the Consul General of Miami was coming to Barbados, I contacted him about this matter and he said he would raise it with the Attorney General (AG) but when he came back, I contacted him and he said the AG said he would investigate the matter. Nothing happened.

I do not know if it was the following year or the year after that, someone informed me that my case had been called up in court on two (2) occasions but it was put back because I was not there. I was never contacted by anyone from the court or police with regard to the case, otherwise, I would have taken a flight and made sure that I would have been in Barbados.

I was shocked to find out, really, that I was not contacted. Again, I sent a letter and another email to the Director of Public Prosecutions to make her aware of what I had heard. To this day, she has not responded. This was a frustrating and embarrassing process. Coming up to the last election, I decided to write a Press Release to inform everybody of what was happening.

Subsequent to this, matters involving people who had similar cybercrimes were investigated and there was an outcome and nothing was happening to my case. I sent that Press Release to a friend of mine, seeking guidance and somehow or the other, not somehow or the other, I know the path it took. It made its way to the Attorney General.

I presume he felt he may have become embarrassed by what was being exposed and the next morning, probably before 10 a.m., my sister was able to call me and tell me that the police from the Holetown Police Station called her, wanting to know how soon I could come to Barbados to attend court. I said all of that to say we went to court but up to this day, I do not know if all of that was to appease me because the case was adjourned and up to now, nothing has happened.

Mr. CHAIRMAN: Miss Cole, Miss Cole, hold on. I just want to say is that you have two (2) more minutes. What you are saying, Madam, is of interest. Obviously, you are speaking about the Barbados Police Service. Realise that this is a legislative body and we are speaking about the Bill, so we really do not have oversight over the Barbados Police Service. We are giving you a little width, Madam. But also, you know, I want you still to focus and realise that your time is running out because Members can also engage you after you speak.

Ms. Heather COLE: The reason why I stated all of that is to say that the law, the cybercrime law, that existed then and the one (1) that is being proposed now that was just passed, offered me no protection; either of them. There is no protection from bad actors in the Civil Service or the Parliament or wherever.

So the old law offered no protection. I read the current one (1) and it also has not addressed the issue. It offers nobody in a similar position any protection at all. There is no guarantee that they will have a day in court.

In conclusion, I oppose the Bill in its present form because it may have significant changes that would affect our Constitution as it relates to freedom of expression. The idea of mass surveillance or detention centres should not be tolerated in Barbados at all. That is my presentation.

Mr. CHAIRMAN: Thank you, Ms. Cole. Any Members wish to engage Ms. Cole on anything she said or otherwise? Ms. Cole, you on at least two (2) occasions said that this Cybercrime Bill, will curtail the constitutional right of freedom of expression. Yes, there is a constitutional right to freedom of expression but is that not right curtailed and, you know, surrounded or ring fenced by certain obligations and limitations, that yes, there is a constitutional right to freedom of expression but that right is subject to public interests, morality and laws of privacy? Is that not the case? So, if that is the case, why are you saying that it threatens your constitutional right to freedom of expression.

Ms. Heather COLE: So, in my opinion, nothing was wrong with the previous Bill. To me, what it does is that the reach of this new Bill is wider and all it can encapsulate many other things that relate to people's

freedom. I think that if the previous Bill had some areas in which it was not up to standard, that it should have been updated but this one is way too wide and vague. Even if we have to try to discuss or try to figure out what freedoms of expression are at this stage, we have a problem.

Mr. CHAIRMAN: Okay but have you seen Section 19 (5) of the Bill?

Ms. Heather COLE: I had it up here. Is there something specifically you wish to tell me?

Mr. CHAIRMAN: No. The Cybercrime Bill, Clause 19 (5).

Ms. Heather COLE: I did read it.

Mr. CHAIRMAN: Which says that they are defences to an allegation of breach of the Cybercrime Bill. Defences that are similar, the same as in defamation, are carried forward in this Bill. In other words, if what you are saying is true and if what you are saying is trivial; that you have a defence to a charge on allegation under this Bill. If what you are saying is comment. Why do you believe that, you know, your constitutional right to freedom of expression are being breached, when you have those defences? You got to be sure, for example, that what you are saying is true. Not because somebody is a politician that you can say any and everything about them; that they are corrupt.

"XY is a crook. He took bribes and even bringing in their mother, as a lot of people do." "What you expect about X Y? His mother was a prostitute anyway, so you cannot expect nothing better from him." Then you cannot prove either of those; do you think that because you have a constitutional right to freedom of expression, you should be able to say that about an individual or their mother; when you cannot prove that it was true? Just using an example.

Ms. Heather COLE: Go ahead.

Mr. CHAIRMAN: Just using an example. You believe that because you have a constitutional right to freedom of expression, you should still be allowed to say that without any penalty?

Ms. Heather COLE: I do not believe in abusing my constitutional rights and I do not think that anyone should take it lightly, as well. I do not publish or write anything that I do not think is true nor that anything that connecting the dots, would not seem true. I would never do that. For example, if I can bring you right back to this very Bill, if you were a lay person who is not familiar with the law and you read this Bill, as I did, and you read 23, 24 and 25, there is something missing between 23, 24 and 25 and it does not make any sense.

So, that is why my query is the surveillance and detention centres because I read it and to me it "ain't" look right; something wrong there. So, that is why I am querying that. To reinforce it, I am not a person who goes "willy nilly" trying to put things on the internet that do not make any sense and that are untrue. Well, perhaps some people do it and if they do, yes, I agree that there should be a law for defamation. That is what I believe. Again, when I read this Bill, the premise that came over is that you are guilty until you have to prove your innocence. Normally, it is the other way around.

Mr. CHAIRMAN: No, Madam. No, Madam.

Ms. Heather COLE: That is the impression I got.

Mr. CHAIRMAN: The time old standard of law and rule of law in Barbados is that you are innocent until proven guilty beyond reasonable doubt. There are a few exceptions to that. I mean, I think possession of drugs. I am an attorney-at-law, Madam and Senior Counsel (SC). There are three (3) other lawyers in this room at the level of King's Counsel (KC) as well; Leader of the opposition; another accomplished lawyer and a top legal drafter, Madam. This Bill does not shift the burden of proof and it is still that any allegation before the court for any of these provisions has to be proven beyond reasonable doubt. So, do not be worried about that.

Throughout the Bill, it speaks towards intentionally or recklessly. In other words, you have to have the mental; the *mens rea*, we call it in law, to commit the offence.

Ms. Heather COLE: So, what is reckless then? If I call somebody a fool and they are not a fool, how reckless? How would you quantify reckless? How would you quantify that in terms of a scale of recklessness?

Mr. CHAIRMAN: We have judges, Madam. You could appreciate; the judiciary will weigh the evidence, *et cetera*. But, if you call someone a fool and I am just engaging you a bit, Madam. I mean, this is not a legal class; a law class. But, if you call someone a fool, a court might very well say that that is trivial. I mean, it is within the context, Madam, of why you call them a fool. That is truth. But, a court might say that

is trivial. Right? That is the defence as well, under Section 19 (5). So, as I said, Madam, it is not a law class we conduct in here. We want to engage you and have your thoughts.

But, I just felt that I needed to ask you that question on the freedom of expression. Okay. Are there any other Members who would wish to engage Ms. Cole? No. Okay. So, Ms. Cole, we thank you for your citizenry. You are a part of our diaspora in New York. I assume you were born in Barbados. You speak like us.

Ms. Heather COLE: Yes.

Mr. CHAIRMAN: So, we thank you for taking the opportunity to give your evidence. Okay.

Ms. Heather COLE: Okay. Thank you. Have a good day.

Mr. CHAIRMAN: Okay, so bring on Mr. Weekes. Mr. Weekes, Good morning, can you hear us? Hello good morning Mr. Weekes can you hear me

Mr. David WEEKES: Yes, Mr. Chairman, can you hear me?

Mr. CHAIRMAN: Yes, we can hear you clearly Sir. Welcome to the Policy and Governance Committee, Joint Standing Committee of Parliament. We have here six (6) Members of the Committee. Six (6) out of the seven (7). We have the Honourable Leader of the Opposition. We have Senator Walters; The Honourable Senator Lindell Nurse; Mr. Peter Philips, Member of Parliament; Senator Gregory Nicholls and myself, Edmund Hinkson, Member of Parliament.

You are permitted for the next 10 minutes to speak on the Cybercrime Bill on the Mutual Assistance in Criminal Matters Amendment Bill; on both of them. As to what you think of these Bills; if you feel that they can be improved in any way your comments on them, Sir. After that 10 minutes any Member can engage you or question you on anything you have said. So the floor is yours.

Mr. David WEEKES: Before we start, Sir, might I inquire of you just as a bit of background. Why was it that other presenters I recall one (1) of the Government presenters make a presentation for almost two (2) and half, almost three (3) hours and individuals who are responding are only limited to 10 minutes?

Mr. CHAIRMAN: Sir, we have rules. Mr. Weekes hold on. Your 10 minutes has started and this is the Parliament. The Parliament of Barbados makes it rules. Can you state your name for the record, Sir?

Mr. David WEEKES: My name is David Weekes.

Mr. CHAIRMAN: Okay and what is your occupation?

Mr. David WEEKES: I am a retired individual.

Mr. CHAIRMAN: I just wanted to be clear, Sir. You said in requesting…

Mr. David WEEKES: You are cutting into my 10 minutes. Will I be allowed to present for the 10 minutes?

Mr. CHAIRMAN: Hold sir, Yes. I said that. You said in your request for an oral presentation that you live in exile and I just wondered what is meant by that because I mean I thought we are a free society and you are living in

exile. I just want you to clear up on that. What do you mean by living in exile, Sir?

Mr. David WEEKES: Mr. Chairman, just to be clear. I want to know whether that query can come after I make my presentation?

Mr. CHAIRMAN: No. No. Your 10 minutes has not started yet, Sir, so just for the record, what you mean by living in exile?

Mr. David WEEKES: I live in a circumstance where having been fire-bombed in Barbados for a particular matter. My matter being that I brought the Governments of CARICOM, 13 Governments of CARICOM to the law courts of Barbados and sought there afterwards to get a trail to proceed for 17 years. Then I found myself fire-bombed, so I live in exile because I do know that if I do come back to Barbados, I will either be incarcerated for the different things that have been constructed to make sure that I find myself in prison or I will be killed. The first attempt failed, the fire-bombing failed so I am here living in exile because of that explicit reason.

Mr. CHAIRMAN: Okay, Mr. Weekes. The floor is yours.

Mr. David WEEKES: Let me just start by saying that you would be very familiar with a quotation from Julius Caesar, sorry, from Romeo and Juliet, "A rose by any other name would smell just as sweetly." What is presented in that statement is that what one says and the actuality, irrespective of what is projected as an outcome; what ultimately obtains is defined by virtue of the outcome. Quite simply, it looks like a rose. It smells like a rose but what we are being shown here are the petals of the rose. I am among many individuals who would caution Barbadians and reviewers alike to consider the petals of this rose that is being presented to the people of Barbados, under the context of the Cybersecurity Bill.

There are some words here that masquerade within that Bill and attention should be bought to those. "Annoyance, inconvenience, embarrassment, insult, humiliation, intimidation and anxiety." On the one (1) hand, they are justifiable issues that the Bill addresses, namely illegal and reprehensible acts that require the enactment of the laws to protect the rights of citizens, politicians and as such.

I guess politicians are a subset of the citizens of Barbados but I respectfully suggest that the new Republic in proposing State endorsed threats and it both denies the rights of the Freedom of Speech. Forgive me saying Freedom of Speech, I should say Freedom of Expression because Freedom of Speech obtains here in United States of America (USA). Freedom of Expression is what obtains in Barbados.

The Budapest Convention has certain provisions and by extension, the Cybercrime Bill purportedly established based upon the Budapest Convention gives those three (3) categorisations of substantive law, procedural law and international cooperation as a matters related to cybercrimes but reviewers would see how definitely the reasonable parameters of the Budapest Convention are exceeded by our indigenous Cyber Security Bill, particularly as defined by Clause 20, Cyber Bullying.

Under 21, it will read in part and I will just give an excerpt:

"A person who intentionally uses a computer system to publish, broadcast, or transmit data that is that is offensive."

I am going to put those words which are important for my representation. *"Offensive, pornographic, indecent, vulgar, profane, obscene or the menacing character or causes any such data to be so sent for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety, or causes substantial emotional distress to that person"* and the Bill continues.

You all have it in front of you and certainly anyone can read it and so forth but I am making focus upon those particular words. I respectfully suggest that there is a disingenuous concatenation of these words being relied on here. The blindest man on a trodden horse can see what the words danger, injury and hatred can refer to but consider those other appended words in the lesser indeed even puerile impact. Annoyance, inconvenience, embarrassment, insult, and said other vapid terms. I respectfully suggest that there is a disingenuous concatenation here being relied on.

The Bill has purposely mentioned danger, injury and hatred with a hodgepodge of words of lesser, indeed puerile import and I would not go over them again. I know that you all are familiar with them. You all wrote it, annoyance, inconvenience, embarrassment, insult, and similar words.

These delicate, emotional and sensitive words which are not criminal acts but like the privileged exchange of *"your mudda",* uttered in the Lower House, might at best be subjectively inflammatory and it raises the question of why have they been included and added here?

I am reliably informed, not to say begs the question here but rather it raises the question. It raises the salient question, "why are these words so purposely being intertwined?" "Why use danger, injury, hatred with annoyance, embarrassment, insult or inconvenience?" I will attempt to ask that same question and say that this concatenation is purposed to create a situation where its artful juxtaposition will be used by parties who seek to entrap the victims of the Republic.

Now let me repeat that part - the victims of the Republic. No defendant charged under this law will be able to delink those emotive words and will find themselves incapable of decoupling danger and injury, from their charges and in anticipation of upcoming questions, I expect that the question will be posed about if I want to delete injury and danger from the Bill and I pre-empt that question by saying 'no' But I suggest, respectfully, that as the Bill is purposely written, citizens have to take all the words or none. Therein lies the petals of this cybersecurity rules of any other name, Mr. Chairman.

The subtle undercurrent of this Bill is that it ostensibly states that Barbadians are free to transmit data as long as it does not defame others but more specifically, while defamation is provided for in existing laws, this now includes a purpose puerility, expanding on the plurality of unnamed distresses, appended to catch any and all dissenters. In a recent exchange, I remember another presenter made a hypothetical example of defamation, made the statement where a fellow would call another's mother a prostitute. I believe it was you, Mr. Chairman, who talked about another giving an example of a mother being a prostitute.

So in a tangential vein, I would like the Committee to consider this example, which would not use the vulgarity that one (1) Member of the House directed to another Member, referencing the mother's parts -- under privilege, of course. Let me give you this tangential banter: Suppose you and I, Mr. Chairman, we were to attend a hypothetical nightclub and you or I spread news of the other individual's dalliances to third parties.

One is led to wonder if that truth being shared to third parties, while not causing danger or injury under the Bill but causes annoyance, embarrassment, humiliation and generally discommoding either of us, if that will be given the expansive or if given the expansive definition of this Cybersecurity Bill; it will activate it and cause either of us to be brought before the Barbados courts by the other aggrieved party because of embarrassment; because of annoyance.

For such a query, I would answer yes and I will go on further to say this, that depending on who we are as the aggrieved party because of the puerile emotive conditions expressed within the Bill; as the aggrieved party, notwithstanding the truth of your seeing me in Frontline or any of those nightclubs, I can easily seek to bring my matter or you can easily bring your matter before the court and though you only embarrass me; you or I can find ourselves guilty of the immature provisions of the Barbados Cybersecurity Bill because my remarks are offensive.

Listen to this: Seven (7) years or $70,000 because I offended you or you offended me and our nation has been silenced from any type of dissent. So this Bill has used two (2) death concatenations which co-mingle legal issues with subjective feelings claimed by an aggrieved party. For example, a politician or their friend; parties now protected by Barbados' equivalent of Thailand's *lèse-majesté,* enacted by a sympathetic magistrate.

I beg your forbearance and this is where I had asked and I really and truthfully had wanted to close and give a simple example to underscore how this fickle annoyance condition under the imminent Cybersecurity Bill can be enacted.

I need your assistance, your Information Technology's (IT) team's assistance, just to make something come on stream and then there afterwards tie in the offence; tie in the issue of how someone can be annoyed by something that underneath this particular law and can seek there afterwards to put me in front of a court or anyone who in similar vein, seeks to make representation or express an opinion which is not a popular opinion but merely because of what you are presenting; it causes annoyance, it causes insult, it causes humiliation.

I wondered whether the Committee would allow me to make representation here and do that if only for a couple seconds. I do not know how much more time I do have but I am finished on this particular point.

(*At this point, there is back and forth as Mr. Weekes attempts to share a screenshot with the Committee. Following instructions, Mr. Weekes does manage to share the image which the Chairman instructs him to take down*)

Mr. CHAIRMAN: But Mr. Weekes, we are not going to allow you any such sharing. We are here to discuss the Cybercrime Bill and the Mutual Assistance in Criminal Matters (Amendment) Bill; so we are not allowing this, Sir. Please take that off. Is your presentation at an end? I need to know on the Bill itself, Sir; that is what we are dealing with.

Mr. David WEEKES: The point that I was finishing on is on the Bill itself; where someone makes a transmission via the computer and underneath the Cyber Security Bill, someone makes a presentation and when they make that presentation or they transmit this information, it causes someone who receives this, to feel annoyed, humiliated.

Those puerile words; that is what I would like to be able to address. I made this specific representation to say that, yes, where there is danger; where there is injury; where there is defamation: Cap. 199 of 1997 provides for those things but to the degree that there is an aspect where someone makes a representation that brings in those other verbs and words such as annoy, humiliate and the such like, Mr. Chairman. Those are the two (2) points I wanted to make here. One (1), to indicate that you do have situations where when interpreted by particular parties, can and will be interpreted in such a way which denies individuals the right of free speech and free expression.

Let me say free expression because I heard one (1) of the Committee Members say that there was no such provision underneath the laws of Barbados but free expression is provided for under the laws of Barbados. On that note, Mr. Chairman, I am sorry to have mentioned things about frontline and so forth. I do not mean to intend any affront to anyone, if I mentioned things that would be disturbing but just to make those examples.

There is one (1) final point. We are moving very slowly towards Thailand's lese-majeste. As nicely as this thing is patterned and as nicely as it is presented, as I said, *"a rose by any other name would smell just as sweetly".*

These verbs and words are the petals of that rose and I would beg that greater consideration be given for this Bill. It be rescinded and a new Bill be presented that is much more harmonious of the rights of free speech and free expression of Barbadians, citizens and persons and residents living within the fair country of Barbados. On that note, Mr. Chairman, I thank you very much for allowing me to make this presentation.

Mr. CHAIRMAN: Thank you, Mr. Weekes. Any Members wish to engage Mr. Weekes on anything he said or otherwise?

Mr. R. A. THORNE: Yes.

Mr. CHAIRMAN: Honourable Leader of the Opposition.

Mr. R. A. THORNE: Good Morning, Mr. Weekes.

Mr. David WEEKES: Good Morning, Mr. Thorne.

Mr. R. A. THORNE: If you called me Ralph and I called you David, would we still be allowed to go on?

Mr. David WEEKES: I am not sure. The Chairman will decide whether we will be able to speak in that particular way but I will address you

as Ralph, if that is allowed by the Chairman, most assuredly.

Mr. R. A. THORNE: Yes. I make bold to say that for both of us this is a personal delight. Yes?

Mr. David WEEKES: Yes.

Mr. R. A. THORNE: Good. I wanted to ask a few questions because for me, this has become a process of my own education and that is why I am pleased that someone of your quality has visited the presentations. So, I am going to ask some simple questions, so that at the end of this exercise, I would have a clearer idea as a Committee Member, as to what is the substance and essence of the objections. I think I know what they are but I want to seize this opportunity, David, to inquire of you by a few simple questions. I take it you are opposed to the Bill?

Mr. David WEEKES: Very much so.

Mr. R. A. THORNE: Good. I take it you are aware that this law, in its form as drafted here, has been passed in other jurisdictions? I do not ask that to excuse what is being done by this Parliament. It is a series of questions that I think is probably the Socratic method by which we will arrive at some answer, ultimately, as to whether the Bill has merit or not.

So, I am just asking, permit me to ask these questions so that the discussion and/or understanding of the discussion will make some progress as between all of us. So, these are simple questions.

They are not tendentious in any way; I just want to be able to come to a settled view. Not as to the nature and content of the Bill itself but I want to come to a view as to what is the protest. What is the nature of the protest out there in the public? That is what I am trying to do. So, I am not being tendentious. I am just seeking what is the state of mind of people who object. You are following me, David?

Mr. David WEEKES: I am following you, Ralph.

Mr. R. A. THORNE: Good.

Mr. David WEEKES: I would not be presumptuous to speak on the public but within the small category of persons who I converse with, both within the diaspora and there in Barbados. The concern is not so much the ambit of the law that other countries that have passed this law. The other countries that have passed this law that they have made provisions for but more so the subtlety. The subtlety within which, if I have offended you: if by mere substance of something that is conveyed via the computer and that is why I sought to use that particular example that I provided, that the Chairman asked to be taken down. I sought to say if the sentiment of individuals is that their rights and privileges that were normally part of these fields and hills beyond recall in Barbados; they seeing that they are being taken back that if someone opens their mouth and says something like, "Mugabe land" and compromises a little meme; you can actually see….

Maybe, I should ask the question, do you not see Ralph, the Chairman did in actual fact give you the KC as opposed to the SC? But, do you not see where there is room for an interpretation or misinterpretation, where such a meme could be brought into the court because it causes annoyance or it causes humiliation?

Mr. R. A. THORNE: We are all always entitled. I am sorry. We are all always entitled to subjective interpretation. The court ultimately has that duty. I want to say to you, David, that there is this saying, *"two wrongs don't make a right"*. So, do not allow that to influence your answer.

My question to you had been this. How does it appeal to you, that other countries may have or have in fact passed similar legislation? How does that influence your argument?

Are you going to say two (2) wrongs do not make a right? Are you going to say that there are peculiar circumstances in Barbados that militate against the passage of this law? Keep an open mind on it. I certainly have an open mind. I can promise you that.

Some of the protestations and objections, I find highly persuasive. It does not matter to me that other countries have passed the law. I am concerned about the passage of the law here. So, I am asking you, how does it appeal to you that

other countries have passed the law? Will you say two wrongs do not make a right? You are muted. Oh, sorry.

Mr. David WEEKES: You got muted. You got muted just now.

Mr. R. A. THORNE: I beg your pardon. I was asking, how does it appeal to you that other countries have passed this legislation?

Mr. David WEEKES: My position is this, Ralph. While other countries have passed that legislation, I do not believe that that weighs upon a "Bajan"; a Barbadian. Any Barbadian who has come up in Barbados where our naval string is buried should not be subjected to such a pernicious law which, by cover of night, is taking away the basic rights of individuals to speak because what I have been hearing is that when you are within groups of individuals speaking in the context of Barbados, now there is a fear merely to write something within the computer format because individuals can send that to a third party and if the law is passed, it be construed a chapeau underneath which individuals can be tormented; sorry can be prosecuted under that law. So I am not really interested in what happens elsewhere. I believe that as Barbadians we have a right to preserve our cherished freedoms.

Mr. R. A. THORNE: The other question I want to ask is this and I think we are leading up to this point and perhaps you have said it yourself; that law must exist in its own peculiar culture and let me say in its own peculiar political culture. That if you have a culture, well you have this law which allows a prosecutor to be fairly selective. You following me?

Mr. David WEEKES: Yes.

Mr. CHAIRMAN: Any criminal offence. The offence of murder takes place you know who to charge. The murderer. Breaking and entering takes place; you charge the person who broke in and entered. Sexual assault takes place; you charge the molester. This offence offers to a prosecutor the opportunity to be widely selective or let us say to be selective because as I have said in here in the last occasion, these offences takes place every minute of every day and you are not going to charge 50,000 people who go into cyberspace and commit the offence and a prosecutor has the opportunity to decide who he will charge.

Is that a concern of yours? We all agree that assaulting people in cyberspace is wrong and that they should be some sanction against it. Is it one (1) of your difficulties with the legislation that it permits the State to select those against whom it will charge? Is that one (1) of your concerns?

Mr. David WEEKES: That is my main concern that we have reduced our laws in Barbados; a place which has come through so much. Where our forefathers well particularly as we consider the period just prior to and following our Independence in 1966. We are moving very far away from what the forefathers perceive or what Errol Barrow perceived and those individuals within that cluster perceived as to, *"These fields and Hills beyond recall are now our very own."*

This law or those particular Clauses; those verbs within there, they expressly allow for individuals to take away those rights and cherished freedoms. That is what I am seeing there. A colleague called me some months ago, when this was being contemplated and he says, "You have offended the powers that be. Why is it that these two (2) things are being so aggressively pursued and I said to that individual my matter of 17 years, when I recognised that I have not been able to get a day in court; I said that the only place that I can go to, is to the United Nations (UN).

Now, before we go any further Brother Ralph; when is say UN I am speaking about the UN Human Rights Commission not the UN Secretary General; so there cannot be a situation where people are saying, *"Weekesy making a comment about that particular position"*. You got your rights abrogated. You no longer have rights underneath the court system in Barbados and you reach out to the UN Human Rights Commission and that in and of itself cause further problems.

I would respectfully suggest that when an individual such as myself, will continue to make representations to those bodies and will not pause in making those representations, that it can cause certain parties to be offended and that is the reason that this law is being pushed with such alacrity.

Mr. R. A. THORNE: Have you looked at the Computer Misuse Act which is on the books and has been so for many years? By your comparison, have you looked at the Computer Misuse Act which I think this legislation will repeal?

Mr. David WEEKES: Yes, but look more carefully. You are not necessarily looking at the improvements because let me just say.

Mr. R. A. THORNE: Just let me develop the question and the question is, do you consider that the Computer Misuse Act has served its purpose or has outlived its usefulness, pardon the cliché; has outlived its usefulness?

Mr. David WEEKES: It has.

Mr. R. A. THORNE: Short question, short answers. I do not think the Chairman will allow us too much longer so that if it has outlived its usefulness and that this legislation is intended to replace it. Do you consider that this legislation has gone too far in potentially trampling the rights of citizens?

Mr. David WEEKES: Yes, most assuredly. It has addressed the fact that the environment with computer abuse has totally changed from when those laws were passed but in its enthusiasm and zealousness of particular parties; it has divided itself, what is word? I forget the term about where reason divides itself from justice. It becomes over anxious. It becomes over expressive; over enthusiastic **ultra vires.** It is now going into an area, where it is saying, "Yes, these things need to be addressed because these have changed but while we are at it, let us also look at seeking to make individuals, keep individuals from speaking anymore. They cannot offend anyone.

Mr. R. A. THORNE: Yes, now sometimes we and when I say we, we who are politicians say things rather unwittingly and the Chairman may not mind that I remind us all that he made reference this morning to politicians and I have heard that more than once; this possible view that this legislation may be intended to offer some additional protection to politicians.

I have not heard anyone say priests; policemen; garbage collectors and whenever I hear a reference to a category that suffers abuse; I hear politicians. Do you think that any legislation should focus on the protection of a particular group or particular groups?

Let me ask that differently, do you consider that this Legislation may be intending to give over protection to politicians and I am asking these questions very objectively because I want to get an essence as to how the public feels; the public here and the public in the diaspora. Do you consider that this legislation may be tending to offer particular protection to politicians?

Mr. David WEEKES: I most assuredly do and I again go to a particular the *lese-majeste*, to say it forbids the insult of the monarchy and please note that I did not say it forbids the insult of the Republic but sufficed to say, that Thailand LM Laws are amongst the strictest regulation on free speech in the world, as it relates to that explicit group, that subset.

If you were to say that the law of defamation currently provides for anyone but I am one (1) of the individuals who particularly believe that this law is for the protection of politicians and their friends.

Mr. R. A THORNE: That is a criticism that you make of this legislation? Yes or no? **Mr. David WEEKES**: Yes.

Mr. R. A. THORNE: Thank you very much and as I said, my questions are not intended to be tendentious; not to be taking a view. I want to know what is the view of the public. Mr. Weekes, I thank you very much. We reverted to our surnames. The Chairman was becoming a little concerned at our informality but we can now jointly declare that we have known each other for a certain number of years which we do not wish to disclose and I was wondering if the chairman recognised you as well.

Mr. David WEEKES: We will not go there; relative to the Chairman and his lawn tennis days with his big service and knocking the ball off the court but nonetheless…

Mr. R. A THORNE: Thank you very much, David.

Mr. David WEEKES: Thank you. Thank you.

Mr. CHAIRMAN: Senator Nicholls.

Senator G. B. D. NICHOLLS: Thank you, Chairman. Mr. Weekes, thank you for your contribution. I just want to ask you a couple of questions because I am hearing from you some criticism. You are speaking, as I understand it, about the provision that makes for malicious communications. Correct?

Mr. David WEEKES: I am speaking to the Cyberbullying Clauses 20(1), (2) and (3); that is what I'm speaking to.

Senator G. P. B. NICHOLLS: Cyberbullying, the provision that makes for cyberbullying as we are talking about Clause 20?

Mr. David WEEKES: Yes, sir.

Senator G. P. B. NICHOLLS: So this is: *"a person who intentionally uses a computer system to publish, broadcast or transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene of a menacing character or causing any such data to be sent out for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety or causes severe, substantial emotional distress to that person".*

That is the provision you were referring to?

Mr. David WEEKES: Yes, Sir.

Senator G. P. B. NICHOLLS: Okay and you are saying that this is trampling on the rights that people have?

Mr. David WEEKES: I am saying that certain parts of it; certain verbs that are there included, that they are trampling on rights of individuals. Yes, that is what I am saying.

Senator G. P. B. NICHOLLS: What is that right of the individual?

Mr. David WEEKES: The words that I am speaking about are the words "inconvenience", "annoyance", "embarrassment", "insult". Those are the words. I made the point of putting up my fingers and using quotation marks, the visual representation of quotation marks, to isolate the words that I am speaking about and I am saying that as it reads, the singular interpretations therein arising, while danger is understood, while injury is understood, while hatred is understood. I would suggest, respectfully, Senator Nicholls, that these words "annoyance, inconvenience, embarrassment and insult", those words really and truly have no place within the Bill.

Senator G. P. B. NICHOLLS: So that, a statement made to a person normally outside of the computer context, that is causing annoyance to a person, is that permitted under law or should be permitted under the law?

Mr. David WEEKES: Under the Defamation Act, I am sure…

Senator G. P. B. NICHOLLS: I am not talking about defamation. I am talking about a statement intended to cause annoyance and disturbance and humiliation to a person.

Mr. David WEEKES: You see, in many respects you are asking for qualifier for a particular word and I am again falling back to the point of the interpretations; the subjective interpretation of these words, "annoyance, insult, humiliation". If I defame you, do I defame you by using an annoying word? Do you remember those words, "yah mudda's … that was used within the House sometime back?"

Senator G. P. B. NICHOLLS: You do not have to keep repeating the same point. I am not going to direct you to answer my questions, yes or no, like Mr. Thorne. It is very easy to say that the words are broad and vague, as some people are saying and are subjective but when you are crafting a law, as I should say in the more forensic term; when you are drafting a law, it has to be drafted in a way, I am asking if you agree, that would most capture; the intention of the drafter is to capture the criminal behaviour that you are trying to proscribe within the society.

Mr. David WEEKES: Is humiliation criminal?

Senator G. P. B. NICHOLLS: Humiliation is not criminal in the sense that if I am humiliated by something but if a person intentionally tries to humiliate me by saying something that is indecent, vulgar, profane, obscene and menacing; there are other qualifying words within the context

of the Bill. For example, if a child or children are playing cricket, I am sure you probably might be familiar with the game. If I say that children are engaging in pre-game banter, like "*I gine lick you down tomorrow or we gine get we bowlers to bowl nuff bouncers at you!"* That could be, as you are saying, humiliating or it could be intimidating but will that be reasonable? Will the reasonable man consider that to be criminal? So I am just asking, would you consider that to be criminal?

Mr. David WEEKES: No.

Senator G. P. B. NICHOLLS: Okay, let me give you another example, David. If two (2) consulting adults make a video of them engaging in a sexual act, where they both consent to the making of that video and one of them releases that video to the public or threatens to release that video to the public in order to gain some particular advantage or in order to humiliate them or intimidate them into a particular position; would that be lawful in your view? If it is lawful in your view, how could we craft the language that will allow the State to ensure that people who engage in these acts, some people might think that they are horrendous, some people might not but generally the State does not get involved in the privacy of people's homes or acts between consenting adults.

If it were an adult and a child, that would be a different kettle of fish altogether but then when that video is threatened to be released, possibly to your employer, I mean, people get these kind of emails all the time, these phishing emails and stuff like that and fall victims to the scammers on the internet from all over the world; eastern Europe and some people, places in western Africa.

If two (2) consenting adults make a private video which is shared between themselves and there is some reason that they disagree or the relationship does not proceed in a normal way and, for example, one (1) party tries to gain advantage over the other. Would you find that objectionable to the extent that we should make it a crime? Revenge porn as it is properly called and if so, how would we capture that, other than by saying a person who intentionally uses a computer system to publish, broadcast, transmit data that is offensive, pornographic, indecent, vulgar, profane, obscene or of a menacing character or causes any such data to be sent for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred. How would we capture that?

Mr. David WEEKES: You happen to have presented something there which mindful of the rights of individuals. Revenge porn falls into the area of pornography. What I am respectfully suggesting is that as it presents itself as these individual; within the context of a jigsaw puzzle, we can pick out the parts. This law presents for the picking out of particular parts where you are going to say it does not have to be revenge porn but merely because of the fact that it did in actual fact cause an individual a level of humiliation. So, there are going to be degrees.

I would turn that question back to you and ask, when it was being crafted, was it crafted those explicit situations in mind or was it crafted to say, "let us become pick and podge that a prosecutor can choose which of these words or the plaintiff can choose which of these words to say, it caused me great humiliation?"

Senator G. P. B. NICHOLLS: So, you are saying that a person in our society does not have the right anymore to complain when they are faced with a computer image; a computer broadcast or the transmission of data that is intended to cause some harm to them, some annoyance or inconvenience? So, this is where the intent of the person who posts this information online and who transmits this data; that the person who is affected by it should have no recourse in the law. That is what you are saying?

Mr. David WEEKES: To answer your question, in the way that it is posed because of the grey area that we are dealing with, I would say, yes, you cannot….

SENATOR G. P. B. NICHOLLS: So annoying people by posting and transmitting data by a computer system that is obscene and vulgar, which is in Section…. Let me finish.

Mr. David WEEKES: You realised what you just did.

Senator G. P. B. NICHOLLS: Sir, you made your presentation; I heard you. I am just trying to get clear what you are saying. Right. So, in relation to Clause 20 (1), it is called

cyberbullying. This is the one (1) Clause that you admitted just now that you had a challenge with; cyberbullying. A person who intentionally uses a computer system to do these things, for your view, if it causes annoyance or humiliation or intimidation, then that is permissible because it could be taking it too far. So because it can be taken too far; it should not be a crime.

So, that the criminal acts that can occur will occur because you feel that if you were to use intimidation, humiliation or annoyance, those would be going too far. That is your view?

Mr. David WEEKES: No. What I am saying is that you have saw, again, in picking a number of circumstances. I recognised this relative to the way that the Bill is

written and the comments that come out of the Bill immediately as someone talks about it; somebody talks about pornography and they add a particular subcategory which is going to cause individuals who are listening to it to be justifiably angry and say that the law….

Senator G. P. B. NICHOLLS: Okay, if you are uncomfortable with pornography, I can give another example. I think Mr. Williams may have mentioned that because I am not all about the pornography thing and I am not thinking that is an extreme example.

Mr. David WEEKES: I cannot finish. You are not allowing me to finish, Senator?

Senator G. P. B. NICHOLLS: No. You are accusing me of doing something and I think I have the right to clarify…. Hold, Sir. You are accusing me of taking out pornography and I used the example of revenge porn but let me give another example. I do not have to rely on that. A school has a beauty contest or a beauty pageant, Miss Whatever School; St. Jude's School. One (1) of the contestants faces email, social media posts where, leading up to the competition, body shaming; fat shaming, telling them about the face and stuff; with the specific intention for that person to suffer some kind of anguish, some kind of humiliation or so. Is that permissible? Should that person have no recourse against persons going online with the intention to cause them some kind of humiliation or embarrassment in the beauty show?

Mr. David WEEKES: I will answer your question by saying this. Sir David Simmons, when he was in the Review Committee, presented a two-year-old pornographic piece of material, which he said he was prepared to share.

Senator G. P. B. NICHOLLS: Sir**,** I asked you a specific question.

Mr. David WEEKES: Can I finish?

Senator G. P. B. NICHOLLS: Yes. at this stage, the Members of the Committee get to ask questions

and if you answer the question I asked, we will be happy and perhaps, the chairman will allow you to expand in the end but I just want to answer the question.

Mr. David WEEKES: I was answering your question by suggesting that particular circumstances, when taken in context of the pornography and the cyberbullying; there would be particular aspects of it that I could actually take a specific situation and suggest the same thing to you that you are suggesting to me. If I ask you the similar question, you would similarly be….

Senator G. P. B. NICHOLLS: I asked you two (2) questions. I asked you if a specific thing would be objectionable. If it were objectionable, whether or not it you will be able to get it into the law without using the terms intimidating, humiliation, embarrassment and annoyance which you have picked out as words that are too broad. So, I am asking you, I give two (2) examples and there could be more because we can sit down as a drafter or lawmakers and conceptualise every criminal act that is likely to occur in the future, particularly in something so pervasive as technology.

We are talking a lot about cybersecurity but this is about cybercrime. This is a Cybercrime Bill. In drafting the Bill, you accuse the language of the legislation of being broad. You accuse in your answer to Mr. Thorne's question, that this was being designed in a manner so as to protect politicians; members of the political class and their friends. So, that that is your view. Everybody is entitled to their view but I am asking now, is the language too broad? If the two (2) examples I have said, the revenge porn or body

shaming in a beauty contest or people playing a game of cricket and you are sledging your opponents online as young people would do with the intention of affecting how they perform in the game or something, is that objectionable?

If it is objectionable, in your view, how do you deal with it within the context of cybercrime? Those are just the two (2) questions I am asking. I am sorry if I had to explain the context a little long but that is where I am coming from.

Mr. David WEEKES: I am hearing what you are saying. I am respectfully saying that there are going to be circumstances where, as you have pointed out, that you can have revenge porn and can have situations where the law needs to be able to address but I am also suggesting as it currently is written, your too far East is West. From what I am seeing there, you have gone too far East.

If you want to come down to more specifics, there are other places and other laws that you can depend on and refer to and redraft what is currently there. I am just saying that to have it as expansive as it currently is, it is going to lead and has already started to lead, to the point where dissent is being killed in my fair country of Barbados.

Senator G. P. B. NICHOLLS: I am coming back in because this is my question time. You are making the same point again. I will give you another example. You receiveD an email which tells you that they have some photograph of you in an indecent place or is exposed indecently and you need to make some deposit in somebody's bitcoin account or send some money wired to a particular account. You ignore that email. The email tells you this is the second warning. You ignore it. Third and final warning. Would you agree that that is an email that it has not transmitted anything that is offensive yet, pornographic, indecent, vulgar, profane or even obscene because the image or alleged image has not been disclosed to you at that point in time but under Clause 20(1)(b), this would be for the purpose of causing annoyance, inconvenience, danger, embarrassment, humiliation, intimidation and anxiety. If it did not come under this section as you have just suggested, what other law or provision in the existing law would such conduct by some troll on the internet would that be covered in our law that exists?

Mr. David WEEKES: Part of your example you dropped off a part of your example about the email. I heard part of it but then the transmission stopped so if you would care to just.

Senator G. P. B. NICHOLLS: I am going to try to go quickly. Someone sends an email threatening to release some photograph or video of you say for example, we have a video of you watching porn on the internet and we are going to send it to your work colleagues or your boss or something like that if you do not transmit some money over the internet. That causes annoyance, right? That causes humiliation, intimidation, correct?

Mr. David WEEKES: It is an act of extortion and I am sure that they are laws that provide for extortion currently within the laws of Barbados. Am I correct? You can tell me; you are the lawyer.

Senator G. P. B. NICHOLLS: Mr. Weekes, we are speaking now of the effectiveness of this legislation and it is being coupled with the Mutual Assistance Act which would now allow the court to have some jurisdiction over acts that affect Barbadians even though they are not perpetrated on Barbadian soil because of now the pervasive use of technology. We can talk about extortion but if I say that a Bulgarian national or someone from Nigeria and not meaning to disparage those two (2) countries but those are just two (2) examples that I cite; is making these demands on you, how then can the law relating to extortion effectively deal with that situation?

Are you saying then that the citizens of Barbados who may be exposed to this on the internet, should no longer have or should not have in protection like other societies, which are putting Cybercrime laws in place but because the common law in relation to extortion that has been around for centuries, is satisfactory. That is what you are saying?

Mr. David WEEKES: No, that is not what I have said. I started by saying; my first statement was that there is a need. Do not believe that I am against the laws. They are laws and justifiable issues; that is what I started. In my first three (3) minutes, I said on the one (1) hand they are justifiable issues that the Bill addresses namely, illegal and reprehensible acts that require the

enactment of laws to protect the rights of citizens. I do not know whether you were there, when I was saying that.

Senator G. P. B. NICHOLLS: I was here and I think I can assuage some of your concerns, that I too have my own issues. I have said it publicly and I have said it here in Committee on more than one (1) occasion. With some of the tightening of the language that I think we have and I think on the last occasion, I believe that the law is a start and that this process, this Parliamentary process which is new to us in Barbados, can bring us the best version of the Bill that is necessary to achieve that balance and not because I am an attorney-at-law but I do believe when we do not get the balance right as a Parliament; there is a body that is higher that can rule on whether that balance has been struck and as far as I am aware…

Mr. David WEEKES: That is why Senator, I was saying I have waited for 17 years. That is why.

Senator G. P. B. NICHOLLS: I am not getting into your individual case because we can trade stories. You probably need to get a good lawyer. If you had a good lawyer, you probably would not have had that problem right; so I am not getting into your individual case at all.

Mr. David WEEKES: It is not an individual opinion or is not the part of being invited?

Senator G. P. B. NICHOLLS: You should probably speak to Mr. Thorne but he is bit busy now so you might not be able to get him. One (1) last comment though. You spoke about it in your presentation or back to a point that you made in your presentation about Freedom of Expression and I for one think that the Freedom of Expression we have in our current Constitution is ample and well set out. It is very broad. It is a right that the courts in my view will interpret in a broad and a liberal way as is the norm in interpreting Constitutional Rights and Freedoms. The Constitution does create the Freedom of Expression in those broad terms but it also creates the ability of Parliament to make laws that can be inconsistent with those rights, to the extent that they are reasonably required in the interest of defects; public safety; public health; public order; public morality or that are reasonably required for the purposes of protecting the rights and freedoms of others and that is something that we tend to lose because in our zealous nature to be able to say what we want we feel that we can just trample over the rights of people who do not think, look or speak like us.

I will say again in this Committee, any law that is brought as a limitation on one's Freedom of Expression that comes outside the expressed limitations in the Constitution and these limitations have been adjudged over and over since 1966 when we have had these as permissible restraints on the rights. The test or portionality is the basis on which a court will determine rather a law has gone too far. In our understanding of these rights, I know we might look at the American Constitution where they are no textural or written limitations or rights. Our Constitution creates the right and also permits for laws to be passed by Parliament who makes laws for the peace, order and good government of the land but those laws have to have what we call reasonable restraints and if this Bill is outside of it of those reasonable restraints, then I verily believe that people will not have a difficulty in going to the courts and having the law struck down.

We have courts that strike down laws in Barbados that are unconstitutional. Laws that are passed by Parliament so that this notion that we are now all of a sudden become undemocratic by the mere passing of a Bill; not even an alteration of the Constitution but a Bill, an ordinary piece of legislation cannot take away Constitutional Rights and I think that the view that is being expressed is being expressed to mislead people and the perhaps may not be a proper understanding of the wide scope of Constitutional Rights and their expressed limitations in the very Constitution of Barbados. Thank you Mr. Weekes.

Mr. CHAIRMAN: Thank you, Senator Nicholls. Mr. Weekes, I just wanted to clear up one (1) point here and yes I recognise when you came on you are who I thought you were; my senior at Secondary School. I did refer you know single out politicians but it could be anyone and I want to go back to your statement, "You believe that this Bill is being passed or this legislation is being enacted to protect politicians and their friends."

I could have said public figures because often these days, people go online and are abusive to judges. Judges are not politicians including the Chief Justice so it is always easy for people to say that the politicians are passing laws to protect themselves and their friends but I have seen many times, people on social media abusing people who they may have been in a relationship with a short while ago, saying what Bajans would say "outing them" and they certainly are not politicians. I do not know if they are politicians' friends. Politicians supposed to have friends all around; the constituents supposed to be their friends. So I do not know if you are including them in that but I do not believe you are.

I think that it is a bit unfair and I totally would want to disagree with you that the nature and object of this Bill is to protect politicians. At all levels I see people on social media receive social media posts; people in all categories being cussed and abused and humiliated. I just wanted to put that on record, Sir.

Even though I am getting the impression you have difficulty, not with the principle of Section 19 and 20 but with some of the language in it; contending that some of the language is too vague. As you said in your opening, as part of your opening, you do see the need for this legislation in principle. Is that correct?

Mr. David WEEKES: That is correct, Mr. Chairman and just essentially to say that it needs to be tightened up. There are certain aspects of it that can be abused. My concern is, yes, you do need to do this and certainly to go back to Senator Nicholls' remarks, there are certain things that you need to address. The laws have changed: times have changed. You need to be able to address that.

At the same time, there are certain aspects of this Bill that clearly going to a shade of gray that is extremely concerning to any and all citizens. He, himself, has his reservations about it; I have my reservations and I respectfully suggest that based upon the ambit that obtains relative to justices, who knows who and how specific systems are utilised, leveraged and otherwise abused, that this, what is being contemplated here, it will be; we will live and see but I suggest that this is going into a shade of gray that we are going to go back and we are going to regret; if changes are not made to it in its current form.

But again, I thank you very, very much. I realise that you gentlemen have given me well beyond my 10 minutes. I am most appreciative of this; to make my presentation and to make my points about what should be considered. It is not written in stone; so go back to it; make considerations for the individuals who are speaking about it; particular aspects about it.

Man is not made for the law; the law is made for man. That is the consideration that I am kindly suggesting here, that some review, some accommodations for what are the general concerns of Bajans; relative to their freedom of expression.

Mr. CHAIRMAN: Mr. Weekes, we thank you. At the start, you started to say about how you only had 10 minutes, so you have had 75 minutes. So that is why I told you, do not worry about what other people say. We make our rules, okay? Thank you.

(*At this point Mr. Weekes' Zoom interaction ended and university student Timon Howard entered the Chambers*)

Mr. CHAIRMAN: Welcome, Mr. Howard. You have asked that this Committee, the Governance and Policy Joint Standing Committee of Parliament, to hear you on the Cybercrime Bill and the Mutual Assistance Criminal Matters (Amendment) Bill, as presently drafted. Pursuant to that, we have invited you to come before us and to speak for ten minutes, maximum, on these two (2) Bills or either of them.

After that, any members here can engage you on these Bills. The Committee is fully constituted; all seven (7) members are here at present. You state your name for the records and your occupation.

Mr. Timon HOWARD: I am Timon Howard. I am currently a student at the University of West Indies, Cave Hill Campus and I am a spoken word artist.

Mr. CHAIRMAN: What are you studying at university?

Mr. Timon HOWARD: Human Nutrition and Dietetics.

Mr. CHAIRMAN: Okay, the floor is yours.

Mr. Timon HOWARD: Thank you, good afternoon to one and all. I am pleased to be here. I appreciate the opportunity to come and present before you. As I would have stated, I am a spoken word artist, so I am coming before you today as a performer. I saw it fitting that I perform my duty on oration, not quite the norm but spoken word poetry. So more specifically, as a performer, artist, creator, and the user of the social media.

So I have been following the proceedings from last Monday and this Monday as well. I want to say well done to Janine Butcher; Kemar Stuart; Niel Harper; David Weekes; Dr. Ferdinand Nicholls and I particularly like where Dr. Ferdinand Nicholls said, "*freedom is not the right to do what you want but is the power to do what you ought"*. I think that was a brilliant statement.

The critical function of freedom of expression as expressed from a rights based perspective, is that of a moral right, as the UN would see it; from a non-rights perspective, is moreso viewed as a necessity. Whether it is a necessity to uphold democracy in a democratic nation or to combat government corruption or incompetence, *et cetera*, that would be the purpose of freedom of expression.

A source such as that like Stanford, their department of philosophy would say that a tyrannical state that imprisons descendants acts unjustly, violating moral rights, even if there is no legal right to freedom of expression in its legal system, which is a far contrast from ours, whereby we do subscribe to, you know, freedom of expression as a natural human right and we tend to try to uphold that.

At this point, we also commend this Committee and the Government. In a technologically developing society, it is very important that we develop legislation to suit. My issue is, as you can tell by now, perhaps laying in the nuances related to freedom of expression, particularly in Section 20(1)(b). In Barbados, we have an unfortunate history, particularly of silencing our revolutionaries or forcing them off the island and I can say I fear this may further aggravate that problem.

When I think of persons like George Lamming or Clennell Wickham or when I think of men like Clement Payne; who was a union organiser and a highly effective one (1), as one (1) source says the **Caribbean Beat** magazine. He arrived on the island beset by economic problems and hardship in the wake of the depression. Sugar prices had fallen catastrophically and plantation owners had responded by slashing wages and Payne.

Influenced by the black power ideology of Marcus Garvey and the growing radicalism of Trinidad, he delivered a shocking message that the black and poor majority in Barbados should organise themselves in a union and confront the planters and their allies. Confront them.

Not that Payne advocated violence. His motto was to: "Educate, agitate but do not violate" but he grew big crowds with his speeches to hear fiery denunciations of injustice and deprivation. The colonial authorities were predictably hostile to this firebrand orator and the constabulary warned him that he was under observation each moment of the day and night.

We know that when the labour unrest broke out in Trinidad in 1930s, Payne was eager to tell his audience what the authorities would rather have swept under the rug. The whole of the Caribbean, he said, was on the move and justice was there for the taking. He organised a union meeting; the Barbados Progressive Working Men's Association and at that point, the Government would have taken action and made it absolutely their job to send him back to Trinidad.

You could read more about that in the Caribbean Beat Magazine. When I think about men like Gabby too, you know, I do not know about you but if I was Jack Dear, I would be shedding tears if a man as mighty as Gabby cast stones at me. I risk at libel like he head tear, probably. Jack could get his jacket straight but if Gabby were to have gadgets and posting up to free de beach calling name so freely, I wonder what would happen to he if this kind of thing was passed 1982 or even 1983.

I mean, as it stands now, we could see how soca being hit hard and far away from being hard hitting social commentary. That is why it is just jam and wine and jokes in this country. Libel laws done got things choke up tight, compared to a scene like calypso in T&T; where artists like Cro Cro can sing, express dissent and foul play a bit more freely without being caged. But, I will pause on that.

Back to Dr. Nicholls. He brought something off the press from 2018, when election time was setting and words was flying high and empty promises full of hot air like balloons rising like the bread in the oven at a bakery.

He said this one comes from the Leader of Opposition now, Prime Minister, Mia Amor Motley. Gotta love she! She said, *"Today is about sending a message that the people of Barbados will not allow anybody; neither Labour Party, Barbados Labour Party, Democratic Labour Party and private sector to intimidate; not ever again. You have been raised to think for yourselves and you have the right to speak out and you have the right to speak out without somebody trying, trying to unfair you in this country. So, today is equally about reclaiming for Barbadians the right to express themselves in an environment which is, where fear is removed.*

If ever the time comes that you give us the confidence to lead you, we too must ensure that we never rule a Government to unfair or cause fear in this country. This is the solemn promise of the Barbados Labour Party."

I ain't know about you but if there is an intent to keep that promise, the broadness of Section 20(1)(b) seems unwise. My challenges lie mainly in the philosophical approach to understanding the fundamentals of the importance, invitation and the infringement of freedom of expression; a universal human right, which right now, seems to be being made to bow beneath the guillotine to have a critical piece of its being be removed.

I am dressed in a monotone fashion, for I am prepared, if extremely perturbed and reluctant, to mourn our great loss and much less prepared to pay the great cost. I am not trying to move you to tears. My colleague before, Kemar Stuart, did a good job in asserting that this is not an emotionally guided issue. It is very hard for emotions to be found criminally damning.

But, I would be damned by my own conscience if I say nothing. If a man can say something true or false on socials and because the person impacted by the use of his computer system is intended to be annoyed, inconvenienced, obstructed, embarrassed, humiliated, insulted or feel anxiety, he can be damned.

Mr. Chairman, you have said many times that you are an attorney-at-law. Earlier too, I believe, you said there are other lawyers in the room. Correct? Yes. What is your issue with filing such cases under the coverage of the Defamation Act and leaving it at that?

Establish policy with clear defences instead of allowing a web of ambiguity to be a trap for the judiciary you have constantly kicked the can to. Really? My understanding is that the goal of the Bill, as it seems largely, is to bring improvement.

If the way it is currently drafted is highly able to be abused in the palms of powerful players, where you may criticise an individual in some position of authority responsible to the citizens of this country, for in truth neglect of their duty, they remain not subject to changing their ways but you subject to charge. You may not be able to afford the bond to be unbound before you are found guilty and fined up to $70,000 or redefined from a concern civilian to criminal in your sentence of a term to seven (7) years hard time. I bear all of this in mind.

I also bear in mind that we are all beings with egos and insecurities. To forget this is to forget humanity. To reject this is to embrace a pointless naivety which can only lead to a pitiful existence in a strange form of arrogant, ignorant madness.

I would urge the Committee to not let this negligence nor unbelief consume you. Yes, it states in Section 19 (5) that subsection three (3) of that same section is covered by the Defences of the Defamation Act. However, that not the case for Section 20(1)(b), as far as I see it.

The differences in question being that of truth, opinion or fair comment and privilege. At this point in time, I am open to questions.

Mr. CHAIRMAN: Thank you, Mr. Howard. As I stated earlier, I do not want this to generate into a law class but you have basically focused on Section 20(1)(b). Let us look at it; you have it there.

Now, realise that Section 20(1)(b) is subscribed by Section 20(1)(a). You can correct me if I am wrong but I am getting the distinct impression, you are taking Section 20(1)(b) to stand by itself and to say that anyone who intentionally uses computer electronic device to cause annoyance, *et cetera*, that that is the offence in itself.

That is not what Section 20 is saying. In other words, realise that there is no "or" there. It is not Section 20(1)(a). You are publishing this offensive pornographic material or (b), for the purpose of that like how some sections like 19(1)(a), intimidates a person or (b) threatens…. You following me? There is no "or" there in Clause 20(1) separating Clause 20(1)(a) and Clause 20(1)(b). So, you take them together. In other words, this section of cyberbullying is saying that an individual who intentionally, in other words, they have the mental capacity to do it. They want to do it; they intentionally do it.

They publish or broadcast something that is offensive. In other words, you know, it is not good. My submission coming within the limitation of your constitutional right of freedom of expression, is pornographic. You have had a relationship with somebody and regrettably because I have said in Parliament, pictures of nudity taken, relationship finished and now somebody wants to send these nude pictures of their former partner online; indecent.

I mean, we cannot encourage indecency and there are laws against that profane; obscene; vulgar. You are publishing something that is one (1) of these. Alright. We could argue and debate as to whether some of the words go a bit too far. That is up for debate and obviously the Committee, that is one (1) of the mandates of the Committee to look to see if it is too wide but in doing those things, for the purpose of a causing annoyance. You follow?

It is not that they are disjunctive; they are together and I want to because you are focused on that section so are you saying that an individual who, to use an example here given is, a pornographic 3 o'clock every morning they are getting out of bed and watching a lot of porn movies and no one knows that. That is not known to the public. The public sees this person as some upright person. The person might be a priest doing that but they are an adult and that is what they are doing 3 o'clock on mornings and they and their wife let us say or their husband for that matter because it goes both ways; they break up and now the wife or husband wants to use that against them and publicises that on social media.

To say that this person is a fraud and play that they are so upright in the church every Sunday but up every morning watching pornography. Do you think that that is right and that a person should be allowed to do that, to cause annoyance and again, like I said you might debate that all of these words in (1)(b) are too vague; some of them not all as the previous presenter did. Do you think that they should have the right to do that and to even say look if you leave me, I will do this? I will tell the world because when you put something on social media, you are telling the world. I will tell the world who you really are. I do not mind you. Do you think that it should be allowed?

Mr. Timon HOWARD: I think judging by the reaction of some Members of the Committee, it seems to be an amusing situation.

Mr. CHAIRMAN: Nothing about this Committee is amusing. This is a serious Committee and this is real life. This is nothing no amusing; this happens.

Mr. Timon HOWARD: Okay in my responding…it seemed otherwise from the laughter in the room and I was not particularly leaning towards that aspect of the sub-section either. If it is and you say you are a lawyer and I suppose you would be better able to tell me that is really and truly a criminal offence or a civil matter?

Mr. CHAIRMAN: No, I am asking you, if you feel that someone should be allowed to do that and it should not be subject to the criminal law?

Mr. Timon HOWARD: Right, so what I am saying is that in coming here now that seems

to be a moral offering that you are expecting me to make in terms of my judgement, whether I believe that the person should do that or should not do that. Whether it is or is not a criminal matter I am not studied to know if it should be or not. I would venture to say that seven (7) years or $70,000 for that when the Defamation Act only covers what is it? How much is it for Defamation in the Law?

Mr. CHAIRMAN: Sir, two (2) points here because it has been repeated outside of this Committee as well. When you see a fine and an imprisonment term that is maximum and our Interpretation Act; anytime you see this, this is the maximum.

Mr. Timon HOWARD: Even if it does not say up to?

Mr. CHAIRMAN: No, Sir. We have a top legal draftsperson here and she can confirm what I am saying. No law says up to, alright. We do not write legislation that way. That is the maximum and under our Interpretation Act, that is what it says and that is how we draft it in Barbados.

A judge can for instance say that yes, you are found guilty but I will just reprimand you and discharge you. That is the judicial authority and discretion and we have separation of powers, as I am sure you know between the legislation and the judiciary and a judge can say I am going to fine you $500. In other words, once you are convicted under any of these provisions, it does not mean the magistrate or the judge has to sentence to seven (7) years in prison or has to fine you $70,000.

I want to asway you of that, Sir and when you spoke about the defamation, Sir, it is not a law lesson but I have to tell you for the sake of the records. This legislation; this Bill once enacted, it is proposing to repeal 34 of the Defamation Act which is Criminal Libel; that they will no longer be; Defamation will no longer be a criminal offence, okay. I just wanted to point that out to you to but essentially at least I am interpreting your response that you have not addressed your mind for example, the example I gave you which is what Section 20 speaks about.

It is not that you just look at Section 21(b) in a vacuum and that anything that causes annoyance that someone thin skinned and they cannot take insults and because they cannot take insults they go to a police station and you before the court. It is subscribed by 21(b), okay.

Mr. Timon HOWARD: The repeal that you are speaking of in terms of Article 34 that would mean that the current imprisonment of up to 12 months or fine of up to $2000 I am seeing, would no longer be in place?

Mr. CHAIRMAN: Section 24 of the Defamation act would be repealed.

Mr. Timon HOWARD: Which means that would no longer be the punishment and instead it would be what is being listed here under the Cybercrime.

Mr. CHAIRMAN: Cybercrime is within a certain context by electronic means; computer systems *et cetera*.

Mr. Timon HOWARD: That being said; addressing not only the scenario that you would have presented but the statement you would have made in saying that you are not seeing it in a vacuum while yes, the situation that you would have presented can arguably be justifiably tried and that is okay, they are also other scenarios which also may not necessarily be right to fall under this Act and be tried as such. Due to the broadness as you said of it which we can argue in terms of the word being too broad such as a word like offensive which is very vague and then being backed up by the others of annoyance; inconvenience; trivial things like embarrassment and such, could be cause for concern and I am sure you would probably agree.

Mr. CHAIRMAN: Any other Members? Honourable Leader of the Opposition.

Mr. R. A. THORNE: Timon Howard, that is your name? Yes? I am going to ask your age, not to be discourteous but to make the comment that I am going to make. How old are you? Do not answer. I want to commend you; I assume you are very young and I want to commend you for coming into this forum at your age. It is normally a forum in which you find persons older than yourself. So I want to commend you for the courage that you have displayed in coming here.

I also want to commend you for your mode of presentation, spoken word, which is a very powerful medium. I take it that if you do spoken word, you are reading and that is a part of a crisis among young people. Again, I did ask your age and you were sensitive about answering. I suspect you will answer before you leave, though.

Our young people are not reading and I do not blame young people alone because it is the system; it is the technology that seems to be discouraging reading. I want to encourage you to continue to read. Sometimes you may even consider, young people in this country may even consider, putting down the gadgets for one (1) day and reading. The personal and intellectual discipline that is involved in that is highly developmental.

If you are not reading and you are doing YouTube, for you personally, I would like to recommend the lecture by Akala as a spoken word person, I am sure you know that name. Yes, Oxford Union address. If you have listened to it once; go and listen a second time. You will find that it is extremely helpful in terms of your personal and intellectual development.

So, young Timon, I congratulate you for coming into this environment, even at your tender age. I commend you as well for using the medium that you have used. That takes courage because they do not, they do not use spoken word in here. Yet, you have proved to everyone in Barbados and across the world listening to this, that spoken word is valid. It is a valid mode of communication. We have understood everything you have said. It is very effective; it is very powerful.

So, I want to, as I said, commend you and encourage you to continue spoken word. Many years ago, they used to do it at the museum on Sunday evenings, Adrian Green communicates very, very powerfully. I want to ask you to continue to be a standard bearer for young people and to continue to be a voice that is socially and politically conscientious because coming here proves that you are socially and politically conscientious.

Again, it is something that we are losing among our young people as they get lost in the other spoken word and the other behaviour. So, Timon, I admire what you have done here today and I congratulate you. Would you say your age now?

Mr. Timon HOWARD: No, Sir. Thank you very much for the encouragement, though I appreciate it. I am not sure if there are any other questions particularly related to the Bill itself or the presentation.

Senator G. P. B. Nicholls: Sir, I noticed that the presenter here is an artist and I am particularly interested in whether he had any views as to whether the Bill puts any undue restrictions on artistic licence and if it does, how can we protect vulnerable persons from cybercrime, if I were to say that was not the intention of the Bill, to put restrictions on artists, comedians?

Let me give a little context, comedians would ordinarily lampoon people of the political class; people who are in public life; to the enjoyment of the crowds and the audiences. Let us say, for example, that is put online; televised; broadcast on the internet. Could that be a crime? I doubt very much that that would be the intent of the Bill. Do you see that as a possibility, based on any reasonable interpretation of the Section? And if so, if you have any suggestions as to how we might be able to segregate that from any other of the offending provisions. I am interested in your views on that.

Mr. Timon HOWARD: Thank you very much for that Senator Nicholls, I hear genuineness in that approach and that question. I do see it in terms of us being artists and creatives. As I mentioned, some artists like Cro Cro in Trinidad and here, Gabby and other oral presenters who may not necessarily have always been the softest with the blows or in the approach that they took to addressing certain issues.

As I would have stated before, being in an age of technological evolution, whereby we are using the social media to push the content that we create; the artistic licence that we have, that is something I am concerned about in terms of, due to the words of such as “offensive”.

Yes, there are other things which are very valid and like I was saying before, I commend you all for the Bill and for the Committee itself, like,

as you had used the example of the pornography and such. If it is that you are releasing pornographic content of someone that is obviously and clearly wrong and punishable by law as a criminal offence. I can one hundred per cent agree with that.

When you say something like just transmit data, that is offensive, persons take offence to a lot of things. I mean sometimes persons take a lot of offence to things that are true, right? In an age where it is; I mean we are a democratic society. As I prefaced my piece by stating in terms of the fact that a function of freedom of expression can be thought.

Aside from it being a human right, fundamentally; being human beings, we want to communicate and be able to listen to others and make decisions and process thoughts; but aside from it being a human right, in terms of a functional perspective, maintaining an upholding democracy, persons need to be able to voice dissent.

That is one of the critical pieces of freedom of expression and so, when you say something like, something that is offensive or something that causes annoyance or intended to cause annoyance or inconvenience or obstruction is something that you can be punished for; held guilty for as a criminal offence; and as other persons would have referenced before this, going on your record and affecting you as a person, your reputation, your character, *et cetera*, with no recourse or recompense for that, I believe it is extremely concerning, as an artist.

Senator G. P. B. NICHOLLS: Are you suggesting that we should carve out something for that artistic space? That is what I am trying to get at.

Mr. Timon HOWARD: That would be fantastic. Even if I go about my day and I am not necessarily, you know, performing per se, speech itself, being able to have that dialogue and that discourse; being able to do what we are doing right now and share thoughts which may not be, I do not know if I agree with the lady over here, if she agrees with me; if I agree with the gentleman here, if he agrees with me. He may say something that offends me, you know but at the end of the day, being able to share that on a fundamental level, a base level, is important.

So, yes, for the artist, but also for common people, that you don't have to be able to have a way with words, to be able to express yourself and articulate yourself and have the opportunity to hear other persons as well, at risk of them offending you and at risk of you offending them. That is all a part of communication and being able to process.

Senator G. P. B. NICHOLLS: **...** I want to ask you a question which is touching us on a little bit more fundamental because, as I keep saying, we have to get the balance right and we do not always get it right. There is a view by some in the society whom I have had to engage with, that there is a lot of paedophilia in the society that is hidden; there is a lot of grooming that is hidden, particularly in our schools. We do not want to admit it. There is a lot of extortion and exploitation of young people by adults.

One of the more effective means of communicating with children and young people is through technology and the social media platforms that they use. What has come up to me is that there were a number of suicides in Barbados that have been attached from anecdotal evidence last year, as a result of cyberbullying in the society.

When you get close to family members who are affected by these, friends and so forth, you see and hear these stories but there is nothing really that you can do about it at present. How do we arrest this? There is always, I mean, I go back to what we said to people who look different to us at school when we were going to school and how we treated each other. It would not be tolerated today.

When I was telling my children yesterday how I acted as a prefect at school with juniors in the school; it would not be tolerated today. What is your view, as you are accredited as a young person, how do we manage that tension? At the same time, we need to create a law that protects the vulnerable but at the same time, we do not want persons who are in public life or persons who are in important positions in society, not necessarily politicians but persons who wheel

power and influence to be unaffected by the slightest criticism that might be.

There might be a pastor in a church of a congregation where it is viewed that his influence on the church is too dominant and there cannot be any views that must contend and that kind of stuff. People feel real psychological pressure from trying to move outside the norm of the church and that organisation, *et cetera*. We see this each day. How do we protect these people at the same time without diving in and creating a Bill that, as the Leader of the Opposition says, could possibly criminalise everyday activity? Is it that everyday activity has now become normalised because it is on social media?

Should we allow that as an acceptable norm where we can do the worst, as they would say, on social media because we know that is the media which people hide and communicate where it really is not going to hurt anybody but sometimes it hurts people. I just want to hear your views on how we get our balance right. What is going on in my head is that the Bill is being criticized for good reasons and bad but I want to hear, at the end of the day, how we achieve the right balance.

Mr. Timon HOWARD: Thank you very much. I think you said a lot that we can hold on to, in that, particularly in terms of trying to create some kind of legislation that helps those who are vulnerable without creating other unnecessary vulnerabilities in that sense. I would say that that is definitely something that should be addressed and looked into. I have stated before, I am not studying law so I would say that is the kind of mindset or understanding that then should be carried into the discussions by the persons who are the policymakers; the lawmakers; *et cetera*, who are more on the academic side mentally and background-wise, equipped to then work on policymaking and stuff like that.

I would say it is saddening, as you said, in terms of your suicide rates and such. It is interesting to see the development over the years of society in relation to cyberbullying from it being, "they could just put down the phone", to where it is now that we are actually trying to address it because of the results that we have seen.

It may be a bit sad to see that it had to be at the cost of a few deaths for it to happen. Nonetheless, I am glad that it is that we are at this point now whereby we do see that it is a critical issue to address. How that will happen? I would say that this Board and this Committee rather is a very important part of it; wherever this process goes afterwards.

I cannot necessarily say, "Well scrap this!" I cannot necessarily say, "Alright, so my proposal in my legislation is Article 20 should say...". I cannot necessarily say that. In relation to the child grooming, Mr. Springer here would have given the example before, I believe it would have been Mr. Stuart, I could be incorrect in terms of….

Dr. R. O. SPRINGER: This morning? Mr. Lewis.

Mr. Timon HOWARD: Last week.

Dr. R. O. SPRINGER: Mr. Stuart. Mr. Stuart talked about monitoring. His concern was monitoring.

Mr. Timon HOWARD: Okay. Well, you are talking the right…. But, yeah…. It was to either Mr. Lewis or Mr. Stuart, the example you had given in terms of the child grooming and the example of waiting for a crime to actually be committed.

Dr. R. O. SPRINGER: That was Mr. Lewis this morning.

Mr. Timon HOWARD: Mr. Lewis this morning. Right. Waiting for a crime to actually be committed before it happens. I do believe that there can be programmes then probably instituted in place, so that students have persons to reach out to because in the same way with actual, physical grooming and abuse, sometimes it would be the uncle or whatever it is. My uncle has come by sometimes and then, like you tell the mother or whoever and then they do not believe you or whatever. That kind of stuff and then things go too far.

There are stories that you hear all the time. In terms of that, having programmes that students and young persons can actually reach out to; to actually speak out; being encouraged to speak out with campaigns against this kind of stuff like, no, this is not normal. It is not normal for you to be

getting gifts from a 40-year-old man who was coming by when you were 12 every Saturday and do things to you that you know is supposed to be happening to you and then just give you a gift and say, "But do not tell you mother…". That is not normal. Right.

Being aware, like rating the education and the awareness of, like, this is not okay and you have places that you can go to actually get help when this stuff is happening to you; that will take you seriously; that will investigate and that will actually bring some kind of recourse as much as is possible after, you know, that has happened to you. As much as recourse can ever be gotten, in that sense. That is just one suggestion in terms of….

Mr. CHAIRMAN: Okay. So, Mr. Howard, we thank you for coming. I am sure that I could speak on behalf of all of us to say that we wish you the best in terms of your studies, your future and to encourage you in your talents and spoken word skills. Okay. Thank you for coming.

Mr. Timon HOWARD: I appreciate it. Once again, thank you for the opportunity. Blessings to everyone.

Mr. CHAIRMAN: Okay. So, Members, other staff and Parliamentary Counsel; we are going to break here for lunch and resume 2:15 p.m. Minister Marsha Caddle and I have spoken with the Honourable Leader of the Opposition and we will wrap up these oral hearings this afternoon. You know and then the Other Business we will decide.

Obviously, we are going to have to ask the Senate for an extension of our mandate because our mandate expires, I think, it is this Thursday, 16 May, 2024. It was 90 days from 16 February, 2024 and, you know, so we will deliberate on that issue after Minister Caddle has concluded. Okay, so lunch downstairs, Clerk? Okay. Thank you.

SUSPENSION

On the motion of Senator G. P. B NICHOLLS seconded by Dr. R. O. SPRINGER, Mr. CHAIRMAN suspended the Joint Select Standing Committee meeting until 2:15 p.m.

RESUMPTION

Mr. CHAIRMAN: So we are about to resume in the post lunch session of the Governance and Policy Joint Standing Committee of Parliament. I want to place on record that we have had over 40 written submissions by members of the public both in Barbados and members of our diaspora.

We now have Minister, the Honourable Marsha Caddle, Minister of Industry and Innovation, who has cabinet responsibility for the Cybercrime Bill, here to wrap up our hearings; oral submissions. I think members have agreed that Honourable Minister Caddle would be our last presenter and then thereafter, we would have to obviously deliberate.

Well, first thing we have to get an extension from the Senate who would have referred these Bills to us. The 90-day period for deliberation which the Senate gave us, expires on the 16 February, 2024 expires Thursday this week. That has to be taken into account is that we only started deliberations on the 08 April, 2024 as I said previously, what with the reconstitution of the Senate with a Leader of the Opposition being appointed.

So, Minister Caddle, we welcome you. She is here by invitation, as is allowed again under the Standing Orders which establish this Committee. We give you the floor.

Hon. Miss. M. K-A. CADDLE: Thank you very much, Mr. Chairman. Good afternoon to colleagues, Members of the Committee. Good afternoon to all those who may be joining us from different locations. I want to begin by reiterating my thanks to everyone who has been a part of this work and a part of this discussion. Colleagues from the Council of Europe; Sir David Simmons and the Law Review Commission; Government colleagues in the Ministry of Industry, Innovation, Science and Technology (MIST)and others who have been involved in the Bill's drafting.

I want to thank you, the Members of this Committee but in particular on this occasion, I must thank Barbadians. I heard from a young Barbadian this morning as I was on my way here, I must thank Barbadians who came to give

evidence to the Committee and I was very much heartened by his engagement and his presentation.

I want to thank Barbadians and others who have taken an interest in this legislation and what it means for them, what it means for all of us. It was important for us to facilitate a certain level of understanding as to why this legislation is needed and to facilitate a certain level of input, from the Barbadian people into its finalisation. I thank the Senate for allowing me, even after it passed the House, to pause its debate, in order for us to be able to fully consider all the ideas and inputs by sending this Bill to this Committee.

I also want to otherwise, put this work, Mr. Chairman and colleagues, in context. We have received feedback and I am sure this Committee has as well, from people who say, on one (1) hand, that the Bill goes too far and those who say it does not go far enough.

We have received feedback from those who, on the one (1) hand, are extremely passionate about wanting their data protected and those who question the very provisions of the Bill that are specifically designed and drafted to protect people's data. I paused this legislation, in order for it to come to Committee to encourage us, as Barbadians, to reflect on what we want.

I say that with all sincerity, to reflect on what we want and the kind of world we want to live in. I feel quite heartened and I feel quite privileged, that we have the kind of democracy and parliamentary system that allows us to do that.

I say that to suggest that we cannot determine that we want to fully experience and enjoy all the benefits of technology and living and working and having our being in an online environment and then, pretend that they are not risks and safeguards that must be attached. I fully support the use and the work of bipartisan committees such as this one (1) Mr. Chairman because these matters of security and safety cannot be the subject of political opportunism. Our democracy must finally become more mature than that.

I have been very heartened to see some of the honest conversation that has been taking place. I have to highlight that data and technology are the new global currency and they are also at once the new global nuclear weapon. I do not exaggerate the scope for harm in the area of data and technology; where there are no borders; where action is often invisible, the scope must be taken in its full perspective.

National security councils all over the world, including ours, now realise that they have to contend with this, in a way, perhaps more than they have to contend with matters of physical security. We have, in a matter of days now, Cricket World Cup, starting here, where the world will be in this region and the world will be watching this region. We have to make sure that we have the wherewithal to be able to respond and to protect our people; to protect our systems; to protect our information because that information is the currency and equally the weapon that will be used by those who want to harm us.

I am glad that this Committee and its bipartisan nature gives an opportunity to all sides to show true, evolved leadership by not deliberately mischaracterising the intent and likely impact of the law but by focusing honestly on people's real concerns; many of which are worthy of our reflection.

Again, I thank those people who have brought their concerns to this committee and to our attention. Mr. Chairman, I am not going to attempt to repeat my hours of presentation; first on piloting the Bill and then on wrapping up the debate in the House. You have those presentations in your evidence. I speak to each clause and respond to many comments that have been placed at that time in the public domain.

All I am going to seek to do here this afternoon, is to clarify a few questions that have come to our attention to address some concerns and finally to offer you some suggestions, based on my own reflections on this legislation.

I want first to draw our attention to a global example that we have seen recently. It is a case of Ruby Freeman; a case out of the United States of Ameriaca (US) and her daughter, Wandrea Moss. On 03 November, 2020, Ms. Moss and her mother, Ruby Freeman, sat across from each other in a counting house and began counting the number of mail-in ballots that had come in during the US election due to the COVID-19 pandemic.

At the end of that count, the tally showed that Joe Biden had a narrow lead over Trump, less than 15,000 votes across all of Georgia. Three (3) days later, officials in the State announced an automatic recount that would take place because of the thin margin and Joe Biden at that time prevailed again. Donald Trump then demanded a second recount which, again, affirmed Biden's victory.

In the meantime, Trump and some of his allies began sharing some unproven accusations of election workers allegedly perpetrating fraud. In early December, a month after election day, Ms. Moss learned that a video of her and her mother had been circulating online, alongside what can only be characterised as outlandish interpretations of what the two (2) women appeared to be doing, as they were counting those mail in ballots.

Another video showed Ms. Freeman handing her daughter a small item that was imperceptible on the grainy live stream footage. Some people online accused the two of them of exchanging a Universal Serial Bus (USB) drive which was allegedly somehow meant to be used to manipulate votes. It turns out that the mother had, in that case, been passing her daughter some ginger mints but the conspiracy theory and I am sure all of us know of this case, took hold and took off.

The following week, the man who served as Trump's personal attorney, Rudy Giuliani, told legislators that a video circulating online showed, “Ruby Freeman and “Shaye” Freeman Moss quite obviously surreptitiously passing around USB ports, as if they are vials of heroin or cocaine.” Facebook; on e-mail; by phone; supporters of Trump who were disgruntled, convinced that Ms. Freeman and Ms. Moss had orchestrated an election fraud on a scale that was capable of upending the result of a nationwide election, began assaulting them with hateful messages, often with racist overtones. Shortly thereafter, their addresses were posted online. People started appearing in front of their homes, harassing them and their neighbours. Ms. Moss had been staying at her grandmother's home and people also started going there.

The result of this was that all of this, as one would expect, took a toll on these women's mental well-being. They had to give up their jobs. They had to move from their homes. They ceased going out in public. As a result of this suit that was brought against Rudy Giuliani and others, he was ordered to pay them US$148 million in damages and the matter has been elevated to criminal proceedings against Trump and others.

Now, I start there to put in context the potential damage that we are talking about here. The fact that a video shared online; circulated online and followed by comments and harassment also shared online; destroyed the lives of these two (2) women. I dare say that what they have lost in terms of their reputation and their well-being cannot be recovered; even with $148 million, if they were, in fact, to see any part of that settlement.

I make the point that it was elevated to a criminal matter because I think that in these things and this is what the legislation tries to bear out. In these things, there is a very, very thin line between the civil and the criminal. It is our estimation and it is the experience of many people, that these matters begin to trespass and in fact, trespass wholly in the area of criminal harm, injury and damage.

I also want, though, to put it in further context by addressing the notion, I should say, that anyone who has anything to say, in any circumstance, that may cause a nuisance, irritation or that we might not like, is liable to criminal proceedings under this legislation. I want to highlight and I only repeat because I have done so in bringing the Bill to the House; I believe others have done so.

The use of the word “intentionally” in the legislation, is perhaps one of the most important things that we have to acknowledge. There must be intentionality behind the act, in order for it to stand up to the kind of prosecution that the Bill contemplates.

There is also a certain evidentiary standard on the part of the prosecution, that there are more lawyers in here than I have been than in a small room in a long time. I do not need to tell you that the evidentiary standard is very high. The evidentiary standard that the prosecutor must meet is not just the balance of probabilities; it has to be beyond a reasonable doubt.

The standard for the defence is then, the balance of probabilities. I start there and I will come back to it later in my presentation because I want from the outset to dispel the notion that anything that anybody says, no matter the circumstance and no matter the intent, is the subject or is the target of this legislation that is not the case.

I am sure that everyone in this room has read this Bill over and over and over and understand that there must be intentionality. One must seek and intend to do harm or one must intend to act without thought to the falsehood of the allegations being made. I will come to that a bit later.

I want very quickly, though, to go through just a few of the comments that have been made in the public domain. Some of the claims, I suppose I would say, that have been made with respect to the Budapest Convention; the extent to which it has a certain amount of level of rigor and whether or not it stands the test of robustness, as the Convention that we should follow, with respect to cybercrime. I just want to share a few things with you and with those who might be listening.

There has been this claim made that the Budapest Convention on which this legislation is styled or framed, is not best in class. The notion that there is a new UN treaty on cybercrime coming and that this legislation and the Budapest Convention are at odds with or incompatible with that UN treaty; that is not the case. I will tell you for reference that, I have had many conversations and consultations not just with those colleagues from the Council of Europe, who work on the Budapest Convention but also people who are working currently on the UN Treaty and who have a perspective on the comparative robustness of the two (2) pieces of work and I will not venture an opinion myself but the fact is and it has been documented that there is no incompatibility at all.

The UN Treaty is not even complete. It is projected that it will be finished early August 2024. The UN Treaty is likely to be slightly more limited in scope and in fact, some Member States have already expressed concern that it is too limited in scope in many ways. There has been a claim made that the UN Treaty will be more robust and more expansive where in fact, the opposite is the case.

Nothing in the second protocol to the Budapest Convention will be reflected in the UN Treaty and the Treaty copies the illegal access provisions from the Budapest Convention and so the Treaty in many ways looks like the Budapest Convention for guidance on how it should frame itself. You would be interested to note that since the beginning of the UN Treaty discussions, the pace of countries joining and signing on to the Budapest Convention has been in fact picking up rapidly; so far from countries feeling as if they should step aside and wait for the UN Treaty that is going to be more robust, countries have since negotiations started on that Treaty began signing up becoming signatory to the Budapest Convention more rapidly.

Under the Budapest Convention, you have over 70 countries that are required by law to be your friend; that are required by law to assist in cybercrime matters and that cannot be understated. I will say for the information of the Committee that Grenada recently joined the Budapest Convention. Over the last month, three (3) more countries have signed on and five (5) more are expected to sign on before the end of June. so they are now 73 parties' signatory and 19 that have been invited and invited simply means that these countries have sent a letter, requesting to join and on that basis have been invited.

I also want to highlight something for those who say that the Bill or Convention does not cover this or that or another thing. The fact that somethings might be missing from the current Convention, does not put them out of the question. That is why protocols are added often to these kinds of frameworks. The second additional protocol is just that. It gives additionally; it does not amend what was there but it gives additionally. It gives more options and this is something that I wanted to make clear because I think we need to be able to put to bed once and for all. We need to be able to clarify that first of all, Cybercrime Legislation and the things that present are evolving and that is one (1) of the reasons that they are somethings that are noted that would be amended or changed in the Schedule by Ministerial Order because we fully expect that weeks, months, years from now, the technology

that we will have to be concerned about will have changed drastically.

That addresses the issue of compatibility with the UN Treaty and this notion that the Treaty is so mehow superior, in fact it is not; it is more limited and countries notwithstanding that it is coming by August, remain committed to signing up to the Budapest Convention.

I also need to turn quickly to this question of ethical hacking and it has come up with respect to the claims being made that the Bill should make provisions for this thing that is being loosely framed as something called ethical hacking and I think that we have to be careful about how we define these things. I will say and we are aware, that there are some discussions in various countries; a finding a way to permit different kinds of access, for a public service purpose.

In every country that I am aware of, that remains unresolved and why? It remains unresolved because it is very hard to distinguish this activity from a crime and so, one (1) thing that the law must be is certain. Let me explain for those who may not be previously aware of what I am talking about. Those who have made certain inputs to this conversation have suggested that this practice of ethical hacking is something that is desirable in our jurisdictions and what they mean by ethical hacking is that someone gains unauthorised access to your data or systems, for the purpose of proving vulnerabilities. Unauthorised access.

Now, in a situation like that, the first thing is to understand that the fact that the access is unauthorized means that this person is gaining access and is able to look at; review; save; disseminate data that the State has a responsibility to protect. The question is when an individual gains unauthorised access, who is to say what they have been looking at? Who is to be able to control what they have access to and the very responsibility of the State, to provide citizens individual data, becomes compromised.

I want us to understand that there is a difference between this and what has been commonly known to come to be called, Bug Bounty Programmes. These programmes, large corporations have been a part and they launch these programmes like Microsoft and others; inviting people to access their systems and show vulnerabilities and really it is a way and they reward them. They say, I am going to give you access. You try to break this thing; you try to show where the vulnerabilities are.

Again, in cases like that, the fact that it is a structured programme with constraints takes you out of the realm of criminality; I have said this before. I, the Government of Barbados like most other jurisdictions, cannot contemplate a reality in which we allow unauthorized access. That would make any legislation to protect systems and data, moot and irrelevant.

I wanted to clarify that and also to give the assurance that the notion that there is this widespread ethical hacking that countries have allowed. Private corporations can do what they want. Private corporations can let ethical hackers run all through their information. They will have to answer to Regulations of that State but as a government, we would be negligent in our responsibility to the people of Barbados, to allow unauthorized access wherein a person gains access to our systems and data and your data and then says, "Well, I will show you how to fix this or I will give you back your information, if you pay me a sum of money or if you let people know that I was the one who broke it."

I do not see how in the context in which we are trying to maintain order and people's privacy and security, we can allow that to happen and just to reiterate that this notion that countries all over the world are doing it is incorrect. There was as well a comment related to critical infrastructure and that critical infrastructure systems should be listed in the legislation. I do believe that the systems that are contemplated with respect to Clause 12 are itemised in some measure in the Schedule and critical infrastructure systems are all represented except for those related to hospitality.

A colleague of mine did raise this notion on whether, as a tourism dependent economy, critical infrastructure that is related to hospitality might be itemised and included. Specifying the nature of the critical infrastructures is something that one cannot object to. I mean, the reason that it is able to be amended by Ministerial Order is that we expect that the identification of the critical infrastructure will change. We will set up more different kinds of critical infrastructure. We are

talking about things like hospitals; cell towers and so on and that will change.

There is also the question that came up and so let me clarify that it is itemized; it is specified but also that we cannot consider this an exhaustive list because infrastructure itself; technology infrastructure; telecommunications infrastructure by its very nature is changing and there is infrastructure that will exist next year that does not exist now and so that can be amended at such time as is necessary.

There are those who have also raised the question of placing a positive obligation on persons or companies who are in control of critical infrastructure and systems to put certain measures in place. Actually that is also contemplated under the Convention. It is also capable of being including in other aspects of law. It is the idea that if you are a telecommunications company, a private utility, you have a responsibility to secure the infrastructure that services the people of the country. There can be no objection to that.

I do not know to what extent, you in making your amendments, may want to consider that but it is contemplated under the Convention and it is capable of being introduced in other areas of law as well. I also want to respond to a comment on Clause 21 that relates to cyber terrorism. There is a notion that the provision for cyber terrorism is not sufficiently broad, which is a bit of a surprising observation because it does not include solicitation or what the commenter calls preparatory acts.

Let me say this. A thing does not have to have a particular label, I would say, in order to reach a level criminality. The guidance note on the Budapest Convention on Terrorism criminalises, by the very definition of terrorism; the proprietary acts that are involved.

There are lots of jurisdictions that have separate terrorism legislation and have not included this provision at all in their legislation. I say that to say that I would not be too concerned that we missed or we are unable to prosecute an act of cyber terrorism because we do not explicitly use the language proprietary acts. That is contemplated in our definitions of what constitutes terrorism.

Now to come to Part Three (3), which relates to investigation and enforcement. Again, there was a concern raised and I think that it may reflect a less than thorough understanding of what these clauses relate to. Now, there was a concern raised that these clauses, Clauses 26 to 28 but in particular, Clause 26, allows the State to intercept data in real time. Under this provision, the State cannot intercept data in real time.

We deliberately did not include it in our own legislation, even though other countries, who have worked with the Council of Europe and who are signatory to the Convention, have done so. We did it specifically because we thought that it might trespass too far with respect to persons' liberties. This relates only to the production of data that is specified.

Under this Clause, you are saying exactly what you are asking for to be produced. This provision is widely considered to be so non-intrusive, it actually proves to be perhaps the least problematic provision for most cooperating jurisdictions because it relates to just the production of data that you say that you specify that you are requesting. This Clause does not allow, nor does it elsewhere in the Bill, allow the interception of data in real time.

I have to say, too, that the search and seizure provisions under this legislation, are fully in keeping, not just with what currently obtains, with all other legislation in Barbados but the Council of Europe is doing a study of how countries authorise search and seizure under cybercrime legislation. I found that 95 per cent operate on this system of sworn affidavits and the system that is outlined in this legislation; that is the system that is used. I wanted to clarify that the search and seizure provisions under this legislation, are not at odds either with what is currently done to be able to obtain a warrant; to be able to have sworn affidavits and so on, for access to certain kinds of information in other kinds of crimes.

It is also in keeping with what the over 73 countries that are signatory, also have as their provisions. I want to clarify something with respect to Clause 27 and 28 on data preservation to say that; perhaps I should reference exactly what was the difficulty. So, data preservation is exactly as it sounds. It relates to keeping

information exactly as it was; as it exists at a certain time.

Let me just make reference to the objection that was raised, the observation that was made on Clause 28. Clause 28 relates to the preservation of data for criminal proceedings. What that means is that there is information that you want to be able to further review, analyse, prosecute; you want to be able to have access to it in the form in which it existed at the time and the Commissioner of Police or any other officer designated by him in writing, may make an ex-party application for a preservation order to a judge or a magistrate, where computer data, including traffic data stored in a computer system, is required for the purposes of a criminal investigation and there are grounds to believe that the computer data, stored in the computer system is particularly vulnerable to loss or modification.

The comment is that in the legislation, there is no discussion of the conditions and safeguards for adequate protection of liberties when collecting and storing data in criminal proceedings, including chain of custody. Chain of custody does not enter here because nothing is moving; there is no chain.

All this is saying is if, for example, there is data that is likely to be the subject of criminal proceedings and it is being held in the systems of a telecommunications company; is being held on Dr. Springer's computer or is being held on somebody's flash drive; all I am asking for is that the data not be destroyed. That is all. For example, there are some companies or businesses that may have a system of automatically getting rid of certain stored data. By asking that the data be preserved, I am saying, "Look, do not get rid of this! I am stopping you from getting rid of it. I am not taking it anywhere."

Data preservation is usually a fundamental first step. What happens is, you ask for the data to be preserved so that you can go and get a warrant to be able to further examine the data. The truth is that our level of authorisation simply to keep data in place is a higher level of authorisation, than there is for most countries. In fact, most countries ask for the data to be preserved to give them time to get a warrant to be able to further examine the data. Here, we are asking for a warrant to preserve the data which is actually an extremely cautious approach to the matter of data preservation.

From our review in 40 years of data preservation in the US, these days one does not even have to be a lawyer to make a preservation request. It is simply asking and this is in that legislation, not in ours, it is simply asking that data not be destroyed. It freezes the data in the hands of the provider. It does not freeze the data in the hands of the Government. That is flatly wrong that suggestion. All it is, is failing to destroy and there is no chain of custody considerations because the data has not moved. As an overall comment, I just want to say on the matter of search and seizure that police officers in this legislation, as with all other legislation, must act within the parameters of the existing warrant.

That is true, whether it is a cybercrime or a physical crime. I want to address the notion that somehow the fact of this being cybercrime means that all of a sudden, officers of the law are at liberty or can take all kinds of liberties with people's own privacy and so on. Whatever would obtain in a warrant where you are the target of an investigation. I have a warrant that entitles me to go into your home; to go under your bed; to go into your pig pen; to go into your garage; whatever is contemplated or whatever is outlined in the warrant, is all an officer can have access to.

I want to come now after those clarifications to, perhaps, the part of my presentation that you may find most interesting. I hope that you find it interesting. It is to say this. Notwithstanding, that clearly I believe that this legislation is necessary; it was deemed necessary as far back as 2005 with the Computer Misuse Act. There are other pieces of legislation that address these matters in other ways. As the law said prior to the drafting of the Cybercrime Bill, the crime of criminal libel was a part of the law of Barbados.

Most of you in here would know about Section 34 of the Defamation Act. In that same section, the defences applicable to civil defamation were made to also apply to criminal libel. The idea of criminal libel is not new. It is being brought into this legislation from a place where it already existed.

When the Cybercrime Bill was drafted, criminal libel was specifically abolished and you

would note that in the Schedule to the Bill. We realised that some defamations can be extremely egregious and can be so much so that they go beyond compensation for civil defamation. I made this point earlier in my presentation of the Bill in the House.

We also have to consider that bringing a civil case against a person requires resources. It requires resources and we have to be, as the State, we have to put ourselves in a position to be able to defend all people.

Those two (2) women in the US, if they had not had the full might of the opposing party and the outrage of other citizens behind them; they would have just been another story of two people whose lives had been destroyed by defamation; by criminal libel or by libel. I want us to understand that the law has to be made for all people and it has to protect all people. Simply preserving this area of legislation in the domain of the civil, does not do that. Many of us speak every day to Barbadians who feel aggrieved by something for which they cannot pursue litigation or take any civil action because they simply do not have the resources.

I think it is important for us to understand that raising this or bringing this to the criminal space, first of all, is not new because criminal libel existed before and also is important to be able to protect people. Further, the scale of the damage and injury can be so great that, in my estimation and the estimation of many other countries; it elevates it to the realm of the criminal. The other thing to note and I am sure that you have had this discussion among yourselves before. Clause 19(3) of the Cybercrime Bill which I will spend a little time on, purported to create a replacement for criminal libel but sought in its framing to protect freedom of speech by giving a person the right to put forward any of the defences mentioned in Clause 19(5).

I want us to be clear that these defences matter and that we should turn our attention and the attention of the public to these defences under Clause 19(5). If a person is charged under Clause 19(3) and can prove that he was speaking the truth; he will have, as we all know, a cast iron defence. Truth as the ultimate defence, is one (1) that I do not want us to lose sight of because I do not want us to alarm individuals with the notion that these provisions go against freedom of speech. They aim to protect freedom of speech in the context of criminal libel by the defences that you have reviewed and that the Bill lists at Clause 19 (5).

As I have mentioned before, the essence of the offence in Section 19 (3) is the intentional use of a computer to disseminate information that is false. I reiterate the intentionality that must obtain, as well as the falsehood. I will also say this. I have myself reflected and listened to what has been raised, in particular about Sections 19 and 20, Malicious Communication and Cyber Bullying and I think the first thing to realize, Mr. Chairman and colleagues, is that I think we need to be careful that we are able to have precision and surety with respect to legislation.

I think that we have to be tight, precise and clear in our meaning so that if these matters do reach the Judicial System, that that system and that process also has clarity and that we can know that prosecutions are likely to succeed if they reach that point. It is for that reason that I think that to the extent that we can remove anything that may be framed or considered vague; that we should do so. I want to offer for your consideration with respect to 19(3) and I would love to have your feedback on this because these are my reflections and based on some conversations with colleagues, I would love to hear your thoughts.

I think an Amendment to Clause 19 (3) that deletes the words *"not caring whether they are true or false"* and substitutes the words *"that are false"* and "*causes or is likely to cause a person humiliation, embarrassment or reputational injury is guilty of an offence"* and so on and so in that way, I would delete the words, "ridicule" and "contempt" and if you do not get tired of my voice I could go on later to explain why I have opted to delete certain words or suggest that we delete certain words.

Mr. CHAIRMAN: Minister, can you repeat what you said there?

Hon. Miss M. K-A. CADDLE: Yes. I would offer that we delete the words. This is 19(3) the words, *"not caring rather they are true or false"* and substitute the words *"that are false"* because the injury; the crime; the act in my mind

relates to the falsehood or the falseness if I were to coin a delicate term of the utterance or of the image or statement; rather than the truth because that is a far more, perhaps a broader set of considerations so I would say delete the words, *"Not caring whether they are true or false"* and substitute the words, *"that are false"* and *"causes or is likely to cause a person humiliation, embarrassment or reputational injury is guilty of an offence."* That would have us delete the words, *"ridicule and contempt".*

Mr. CHAIRMAN: Minister, again to delete, *"ridicule and contempt"* and you said to substitute..

Hon. Miss M. K-A. CADDLE: I can share the language.

Mr. CHAIRMAN: And substitute reputational injury, you said?

Hon. Miss M. K-A. CADDLE: Perhaps I should read. Take out, *"not caring whether they are true or false"* and substitute the words, *"that are false"* and following on and *"causes or is likely to cause a person humiliation, embarrassment or reputational injury is guilty of an offence"* and if my reading is correct, it would mean the deletion of the words, *"ridicule and contempt"*.

Now Clause 20 with respect to Cyberbullying, I also think has some scope for us to be more precise and I think that precision strengthens the legislation so in respect of Clause 20(1) Cyberbullying, I would rewrite Paragraph (b) as follows:

"for the purpose of causing danger, embarrassment, injury, humiliation, intimidation, hatred, anxiety or causes substantial emotional distress to that person."

In so doing, I have deleted the words "annoyance, inconvenience, obstruction, and insult" and I have a method to my characterisation of those words. I think that the ones that I am offering for your consideration that we keep, are either able to be defined in law and or have their definition elsewhere in law and so I feel comfortable and I will tell you that I feel that if we separate the fact that I am the proponent of this legislation; I think also the fact that I am a non-lawyer, who is myself understanding and perhaps bringing the perspective of a person who may feel uncomfortable with certain of these words or definitions.

Now, I have to say that it is my understanding and I think we have a responsibility and you in the room, who are lawyers have a responsibility to clarify that the meaning of a word in our day to day lives does not; need not necessarily align with the meaning of that word in law and that often these words have accepted definitions in law but also that these words have an evidentiary requirement. When I say these words have an evidentiary requirement, what I mean is that, you must prove through evidence in the court, what you take these words to mean.

If I say that something has caused me injury, then there is an evidentiary requirement associated with that word injury and so, I think it is also our responsibility for those who may be taking some of these definitions in the lay understanding; to be able to confirm and to be able to be able reiterate that these words have a legal understanding and a legal definition and an evidentiary requirement that must be made in court.

My other amendments Mr. Chairman really just have to do with the organisation of sections with respect to, for example, the word 'intimidate' at Section 19(4) may be a bit out of place because of where it needs to be defined. It may need to be defined in a different place; that it is something that those who are working on the drafting would clean up but substantively, I do feel:

(1) That it is important that we are able to proceed with the protections offered by this legislation but;

(2) that we are also able to present this legislation and preserve this legislation as something that Barbadians can feel protected by and not persecuted by.

To the extent that we have the capacity to do that with amendments to the language but we also have the capacity to improve the precision and the strength of the legislation; then I offer for your consideration, those amendments. Thank you.

Mr. CHAIRMAN: Thank you, Minister. We will now allow members to engage you on

anything that you have put forward or said or proposed amendments you have just put forward.

Hon. Miss M. K-A. CADDLE: If I may just take 30 more seconds; as I look at my notes. There is one other thing that, again, this is the non-lawyer in me seeking to give people some comfort.

I know that the use of the word libel with respect to fines and terms of confinement is understood in law to mean that it is up to; so that $70,000 or seven (7) years in prison. If it would not be redundant, I think it would go a long way to include in the language "up to" because in the common understanding among Barbadian people, people think that a particular offence automatically. I see people smiling so I am assuming that you all had this conversation already; automatically attracts…

Asides

Mr. CHAIRMAN: The Interpretation Act of Barbados speaks to that. So all of our legislation has a maximum fine and/or maximum term of imprisonment but obviously within that, there is judicial discretion. Yes, we went through that this morning. So, even though it generally speaks to 70,000 or seven (7) years imprisonment or both; a judge may say, "I am just going to reprimand you and discharge you. I am not fining you; I am not jailing you." Judicial discretion must be allowed. All of our laws; all of our legislative provisions that penalise, have it like that.

Hon. Miss M. K-A. CADDLE: I am aware of that but I am also aware that with respect to data privacy; data protection and cybercrime legislation; some jurisdictions have opted to include the language of *"up to",* just because it relates to things like speech, things that people do every day and they have found that in those cases, people want to have a sense of assurance with respect to the severity of the fine. So, I put it on the table, being fully aware of the Interpretation Act and fully aware that this is a Cap, in a manner of speaking but I also wanted to put that forward because we understand that there is a certain concern about the level of the fines and the terms of imprisonment. With that, I am finished.

Mr. CHAIRMAN: Members. Honourable Opposition Leader.

Mr. R. A. THORNE: Yes, thank you. Good afternoon, Honourable Minister. I just have some very short questions intending short answers although I cannot tell you how to answer. Would you agree with me that legislation is justified by its social need?

Hon. Miss M. K-A. CADDLE: I do not know how you characterise social need. The need may not always be characterised as social but do you mean as in obtaining to the society?

Mr. R. A. THORNE: Yes. So, you agree with that? Right and I take it then that it must be your position that there is a need in Barbadian society for this legislation?

Hon. Miss M. K-A. CADDLE: Yes, but remember, we are not just talking about Barbadian society; this legislation; cybercrime is borderless.

Mr. R. A. THORNE: Yes, it is but you would recognise that Section three (3) pertains to Barbadian citizens here or abroad.

Hon. Miss M. K-A. CADDLE: Yes.

Mr. R. A. THORNE: So it attempts to capture infractions committed by citizens of Barbados and persons outside of Barbados, if the offence affects the physical borders of Barbados.

Hon. Miss M. K-A. CADDLE: Yes.

Mr. R. A. THORNE: Good. Now, you spoke of the Budapest Convention and I take it we now know that there are other countries that have passed this legislation or intend to pass this legislation, correct?

Hon. Miss M. K-A. CADDLE: Yes.

Mr. R. A. THORNE: It comes from your Ministry, so you are the parent of this legislation, so to speak, of what is before this country?

Hon. Miss M. K-A. CADDLE: I am.

Mr. R. A. THORNE: Excellent. Now, can you then tell this country how many countries have passed this legislation? Approximately, it does not have to be an exact figure.

Hon. Miss M. K-A. CADDLE: Let me first clarify that for our purposes, there is really no such thing as "this legislation". Seventy-threer countries are signatory to the convention.

Mr. R. A. THORNE: That was my next question. So, 73 countries are signatory, including Barbados?

Hon. Miss M. K-A. CADDLE: No.

Mr. R. A. THORNE: Oh, we have not signed as yet? I see. The order is that you have to pass the legislation first and then sign? I see. We have 73 signatories so far, of that 73**,** how many have passed similar legislation?

Hon. Miss M. K-A. CADDLE: Most of those 73 and I only hesitate because you say similar legislation, so let me clarify. All of the States that are signatory, have introduced provisions related to cybercrime. That varies in different ways by having provisions in different kinds of legislation or having a cybercrime Bill or Act and the other thing that I should say is that the Budapest Convention is a framework. It offers provisions that countries accept or not; it offers guidance for how to frame legislation. But there is no wholesale acceptance of a particular format.

Mr. R. A. THORNE: You do know, by now you would, that normally you become a signatory first to a convention and then you legislate what the convention intends. You do know normally it is the other way around? In most cases, a country signs and then it legislates. We agree on that. Could you indicate to us why there's a difference on this occasion?

Hon. Miss M. K-A. CADDLE: That is the nature of this Cybercrime Convention. You see, I believe that the architects of this, the Council of Europe, understanding that this is, for most countries, a brand new area of work, want to give countries the comfort and the capacity assistance, quite frankly, to be able to go at their own pace, to be able to form the legislation according to what obtains on the ground in the country, to be able to get something in place as well, that signals intent, to be able to protect citizens in this way.

The Convention is different from others in the sense that it gives support to countries to get this legislation or similar provisions on their books and then to go further because being a signatory to the Convention does take you further to sign the Convention.

Mr. R. A. THORNE: I see. Alright, we have accepted that this one (1) is unusual, in that, you legislate and then sign the Convention. When we legislate, do the terms of the Convention become a part of our legislation?

Hon. Miss M. K-A. CADDLE: No.

Mr. R. A. THORNE: It does not. So, what then is the effect of the Convention? You have the legislation, which is your municipal or local law, as we call it. Let me ask it this way. Is there a need to become a signatory to the Convention?

Hon. Miss M. K-A. CADDLE: Becoming a signatory and as I said at the beginning, it gives you a relationship. It gives you a community of countries that must become your friend on certain matters. When you are signatory to the Convention, you then have this network of countries that mutually assist.

Mr. R. A. THORNE: Yes.

Hon. Miss M. K-A. CADDLE: Because we have not yet signed the Convention, we have sought to achieve that through the Mutual Assistance and Criminal Matters (Amendment) Bill, which extends mutual assistance in criminal matters. In other words, that countries will cooperate with us for matters of prosecution across borders and so on. That always existed but we have extended that to include cybercrime. If we had gone directly to the signature of the Convention, we perhaps would not have had to do that because that would have been automatic in becoming a signatory.

Mr. R. A. THORNE: Right. Alright. I accept that you become a part of a community and that international community would assist all members in sanctions, so to

speak, implementation or giving effect to the legislation. It is a community of nations giving effect to legislation.

Hon. Miss M. K-A. CADDLE: Yes, and particularly important, evidence and prosecution.

Mr. R. A. THORNE: Yes.

Hon. Miss M. K-A. CADDLE: By its very nature, as you know, these crimes are often being perpetrated against Barbadians by non-Barbadians in other places. And so, we may need to request evidence, we may need to request data preservation from the US, the UK, Croatia or Zimbabwe; that gives us that.

Mr. R. A. THORNE: Has the USA or any legislature within the USA passed the legislation?

Hon. Miss M. K-A. CADDLE: Does USA have cybercrime legislation? They do.

Mr. R. A. THORNE: I mean legislation pursuant to Budapest?

Hon. Miss M. K-A. CADDLE: I believe so but I can direct you to see the full list of the countries.

Mr. R. A. THORNE: Yes. I would want us to be sure as to whether the US is a signatory to the Budapest Convention, insofar as it deals with this matter.

Hon. Miss M. K-A. CADDLE: That is an easy search.

Mr. R. A. THORNE: Yes, please. We have a patient Chairman.

Hon. Miss M. K-A. CADDLE: Yes.

Mr. R. A. THORNE: They have?

Hon. Miss M. K-A. CADDLE: Yes.

Mr. R. A. THORNE: Yes. Excellent. Now, the corresponding piece of legislation which is the Mutual Assistance Legislation, that has been passed here?

Hon. Miss M. K-A. CADDLE: No, that accompanies this.

Mr. R. A. THORNE: Right. Precisely. So that, the US has also implemented that.

Hon. Miss M. K-A. CADDLE: Remember….

Mr. R. A. THORNE: I take it that they have signed which means that more than likely they have passed.

Hon. Miss M. K-A. CADDLE: Yes, but remember that once you are party to the Convention, the mutual assistance is automatic.

Mr. R. A. THORNE: Yes and you did say it was that the US had signed both Budapest.

Hon. Miss M. K-A. CADDLE: Parties to the Budapest Convention, yes. They are ….

Mr. R. A. THORNE: Based on what you told us earlier, if the US has signed, in all likelihood they have passed the legislation.

Hon. Miss M. K-A. CADDLE: The US has cybercrime legislation for sure.

Mr. R. A. THORNE: No. We are talking about the legislation prescribed by Budapest.

Hon. Miss M. K-A. CADDLE: You are characterising this as legislation prescribed by Budapest. Let me clarify. The Council of Europe operates at various stages of support to countries. For example, the Council may interact with a country that already has very robust cybercrime legislation and they are satisfied that the cybercrime legislation is not at all at odds with the Convention and, in such cases, may invite a country to sign on to the Convention because of existing legislation. I cannot say to you in the case of all 73 countries that each one (1) has followed the exact process that Barbados has followed. There are many different processes that obtain.

Mr. R. A. THORNE: I see. What our representative attorney from CPC will tell you is that nobody pretends to invent the wheel. Legislation tends to copy other jurisdictions and you would agree that this one (1) is a copy from other jurisdictions.

Hon. Miss M. K-A. CADDLE: Well, first of all, let me step back to clarify something else.

Mr. R. A. THORNE: Yes. These are easy questions, though.

Hon. Ms. M. K-A. CADDLE: Yeah, yeah, yeah and these are easy answers.

Mr. R. A. THORNE: Excellent.

Hon. Miss M. K-A. CADDLE: So, we had a Computer Misuse Act.

Mr. R. A. THORNE: Yes.

Hon. Miss M. K-A. CADDLE: Right. I can share this with you, if you would like but there are certain offences that are established as offences under the Computer Misuse Act that are simply imported into the Cybercrime Bill. Right? Then, there are others. Remember, too, that the reason that this was a subject of the law review and came to the attention of Law Review Commission (LRC) is that by its very nature, technology offences are changing all the time. We needed to be able to review the Computer Misuse Act and say whether some of these things needed to be updated; whether there were types of crime or types of data or systems that had not been contemplated in that Act.

So, in answer to your question, I am clarifying that if this is a copy of anything, it leans heavily on the pre-existing Computing Misuse Act of 2005 but then, it leans then, too, on the Budapest Convention to be able to update the legislation to make it fit for purpose today in a 21st Century Barbados.

Mr. R. A. THORNE: Yes. So, what we are agreeing then, is that this legislation is much like other pieces of legislation in other countries.

Hon. Miss M. K-A. CADDLE: As most legislation is.

Mr. R. A. THORNE: Precisely, that is the point. So that no one has reinvented the wheel and I take you back to the United States then. You used the word "robust"; a word that I love, actually, in this context. Has the United States been more robust in its drafting or has it been pretty much in line with what the other countries have done?

Hon. Miss M. K-A. CADDLE: I cannot say.

Mr. R. A. THORNE: You do not know? I see. What we have established is that we can say that this legislation is and I am going to use the word "harmonised". In terms of its content, it is pretty much harmonised across the Budapest Convention countries in its content.

Hon. Miss M. K-A. CADDLE: Yes.

Mr. R. A. THORNE: But you will accept, Minister, that there are some variations from country to country.

Hon. Miss M. K-A. CADDLE: As there must be. Yes. There are variations in ours as well.

Mr. R. A. THORNE: Yes, precisely. There are variations in ours because you, as the parent and I like the term, "as the parent of this legislation"; you have considered that there are peculiarities within the Barbadian system that require us to vary from the harmonised legislation. I could rephrase that.

Hon. Miss M. K-A. CADDLE: I think that we have a duty to make our legislation fit for the context in which we….

Mr. R. A. THORNE: Precisely because ultimately, your position must be that the law must operate within a social context.

Hon. Miss M. K-A. CADDLE: That is almost rhetorical.

Mr. R. A. THORNE: Precisely. You do not pass a law that is not and you use the word fit for purpose which is a phrase I do not like. A law must be relevant to its context.

Hon. Miss M. K-A. CADDLE: Yes.

Mr. R. A. THORNE: Yes. That is almost rhetorical, too. You do recognise that when I say social, I include the political. Yes. So, that you recognize that our social context is different from all other social context is in which this similar law has been passed?

Hon. Miss M. K-A. CADDLE: Our social context is in some ways very similar and in some ways different.

Mr. R. A. THORNE: Okay, similar to whose?

Hon. Miss M. K-A. CADDLE: To many other countries.

Mr. R. A. THORNE: Okay right now our Chairman here tells us that Guyana has passed this

law; well not this law. The law within the framework of Budapest; the Budapest Convention.

Hon. Miss M. K-A. CADDLE: Guyana has Cybercrime Legislation.

Mr. R. A. THORNE: Yes. He speaks with some authority when he says that unless you want to disagree with him and Minister, you would I am sure, accept that Guyana presents a different political culture from Barbados, political and social context.

Hon. Miss M. K-A. CADDLE: In some ways.

Mr. R. A. THORNE: In fundamental ways. You wish me to give you some examples then? The Guyana Constitution for example is classically a Republican constitution based on Guyana's peculiar political culture; certainly they have proportional representation which we do not have. If this does not make you feel squeamish, they have a party system that composes itself along racial lines. We do not have that here. You agree with that?

I think we all in this room know that and I do not think you would want to disagree with that. That is the political culture of Guyana; a party system that composes, in which its party composes itself along racial lines. The People's National Congress Reform (PNCR), I will tell you. The PNCR is predominantly black and the People's Progressive Party (PPP) is predominately Indian. You know this.

Hon. Miss M. K-A. CADDLE: My objection or my hesitation is in your framing of composes itself along racial lines.

Mr. R. A. THORNE: Well, the parties are comprised, the PNCR is comprised largely of an African population. The PPP largely of an Asian population.

Hon. Miss M. K-A. CADDLE: Yes, that is correct.

Mr. R. A. THORNE: And that, that composition affects the political culture.

Hon. Miss M. K-A. CADDLE: Is that a question for me as well?

Mr. R. A. THORNE: You can just agree and we will go on smoothly.

Hon. Miss M. K-A. CADDLE: Take it that I am agreeing to all of the preamble.

Mr. R. A. THORNE: Yes, but the Chairman wants you on record you see and it reflects in Guyana, that let us call it that two (2) party dichotomy reflects social tensions within Guyana's society. I hope they are not hearing me for speaking these truths in such a place as this but you would accept Minister that they are tensions between the two (2) political parties that reflect wider social and racial tensions in that society?

Hon. Miss M. K-A. CADDLE: Honourable Member, that is your premise.

Mr. R. A. THORNE: No it is a question. You either agree or disagree.

Hon. Miss M. K-A. CADDLE: Yes, but …

Mr. R. A. THORNE: You are a historian by some merit.

Hon. Miss M. K-A. CADDLE: Am I? Apparently I am not an economist so I must be something. I accept that this is your premise.

Mr. R. A. THORNE: It is not my premise. Those are questions, Minister.

Hon. Miss M. K-A. CADDLE: So frame the question again.

Mr. R. A. THORNE: Do you accept that the Guyana, the two (2) party, well they are more than two (2) but two (2) dominant parties that the two (2) party dichotomy reflects certain and racial tensions? Do you agree with that?

Hon. Miss M. K-A. CADDLE: I think it, yes reflects as in reflects back to the society.

Mr. R. A. THORNE: Precisely and it reflects those tensions that exists between two (2) racial groups.

Hon. Miss M. K-A. CADDLE: I think it reflects a particular dynamic that citizens have to contend with

Mr. R. A. THORNE: Yes, and you would go onto agree then that those tensions of that nature are not present in Barbadian political society of that nature?

Hon. Miss M. K-A. CADDLE: Honourable Member, I do not know what road you are trying to take me down with you but you would be going by yourself.

Mr. R. A. THORNE: Do not be afraid Minister.

Hon. Miss M. K-A. CADDLE: You are free to share whatever premise on which you are operating but I…

Mr. R. A. THORNE: I am not sharing a premise. I am asking some very easy questions.

Hon. Miss M. K-A. CADDLE: I am not sure that I agree.

Mr. R. A. THORNE: I do not know why you are resisting.

Hon. Miss M. K-A. CADDLE: Let me say this. I think that our islands in the Caribbean present by virtue of their race based past all kinds of tensions. I think that in some countries, we have not had a reckoning. We have not had a reckoning. We have not had a reconciliation and that presents in various ways.

Mr. R. A. THORNE: When you say we, you mean we in Barbados?

Hon. Miss M. K-A. CADDLE: No, we across the region and so, we have gone through that process in various levels so it means then that what one might perceive as an absence of race related considerations may not be so. I do not know that you will get me to agree with some of what you are saying but I await the question related to the legislation.

Mr. R. A. THORNE: Yes, I am coming there and we started nicely on legislation and the content of legislation having relevance to its social context. That is where we were and you agreed that legislation must be relevant to its social context, social and political context because legislation as you further agree, is an instrument of political power; people who have political power pass legislation. The Parliament in which you sit; **I do not have any power in there, if I go to court**.

We are back at the question of social and political context and you are about to answer as to whether you consider that Barbadian society and the Barbadian polity, mirrors that of the Guyana society, in terms of its dynamic. We spoke of the dynamic in Guyana and I am choosing Guyana because that is one (1) of the countries that has passed the Legislation and I am asking you if Barbadian society and the Barbadian polity mirror that of Guyana?

Hon. Miss M. K-A. CADDLE: I do not think that any country exactly mirrors and that is by definition what mirrors means. I do not think that nay country mirrors another. I think there are, with respect to certain areas of law, sufficient similarities in countries that means that legislation is applicable or can be made to be applicable in both. They do not need to look exactly like each other in order to warrant the legislation.

Mr. R. A. THORNE: Yes, so we have agreed that Guyana presents as a society with racial tensions and you will agree, I think, that Barbados does not present with identical tensions as obtained in Guyana. I think you would agree with that.

Hon. Miss M. K-A. CADDLE: Somehow I think that I have passed this road before. I mean a few seconds ago. I think I have clarified that the two (2) countries have some things in common and some things not.

Mr. R. A. THORNE: Right, okay. I appreciate the difficulty in which you find yourself so that you will agree that legislation of this nature passed in Barbados, ought not to be identical with legislation passed in Guyana.

Hon. Miss M. K-A. CADDLE: I make no such concession. I do not know on what basis I would say that, that a piece of legislation passed in Barbados ought not to be identical. No, I do not agree with that.

Mr. R. A. THORNE: So your view is that our legislation can safely be identical with that of Guyana's?

Hon. Miss M. K-A. CADDLE: I think, Honourable Member, that you…

Mr. R. A. THORNE: Do not get upset…

Hon. Miss M. K-A. CADDLE: No, I am not getting upset. I am surprised…

Mr. R. A. THORNE: I am asking if you think …

Hon. Miss M. K-A. CADDLE: Please permit me to respond.

Mr. R. A. THORNE: I beg your pardon? Yes.

Hon. Miss M. K-A. CADDLE: So I am saying that you take legislation on its merits. Right? The fact that I may not look exactly like you or walk like you or talk like you, does not mean that we might not both choose to wear the same hat or the same watch. So I am saying to you that what I am sure the Republic of Guyana did in their case, as Barbados did, is to go provision by provision in the Budapest Convention, to consider the extent to which precisely it was suitable for us. That is what we did.

Mr. R. A. THORNE: Okay, all right, let me simplify it. You have not seen the Guyana legislation, have you?

Hon. Miss M. K-A. CADDLE: I have not read it in detail.

Mr. R. A. THORNE: Right and so, you cannot make a comparison between the Guyana and the Barbados legislations, specifically.

Hon. Miss M. K-A. CADDLE: No.

Mr. CHAIRMAN: Honourable Member, I am just trying to see where you are going with it because Jamaica also has similar legislation.

Mr. R. A. THORNE: But I am going to ask some other questions. That is where I am going.

Mr. CHAIRMAN: Right, I know you are focusing on Guyana.

Mr. R. A. THORNE: You have told this body that Guyana has passed this legislation…

Mr. CHAIRMAN: Jamaica and Guyana…

Mr. R. A. THORNE: I am asking questions about Guyana only because you have told this Chamber, that Guyana has passed similar legislation. As to where I am going, I am going where you led us. To make an inquiry about a comparison between Guyana and Barbados. If you had said St. Vincent, I would have asked about St. Vincent.

Mr. CHAIRMAN: You could come to the point because, I mean, it is not on all fours with Guyana…

Mr. R. A. THORNE: Well, that is the answer I want, so thank you very much, Mr. Chairman. I am obliged to you, Mr. Chairman.

Good, you had told this body, Minister, that legislation must reflect a social need and I think you said that there is a need for this legislation in Barbados and obviously, this is a need to protect persons and their reputations. That is largely what we are trying to do here, are we not?

Hon. Miss M. K-A. CADDLE: It does more than that. It is aimed to protect people and their reputations. It is also aiming to protect information and systems. It steps away from the reputational, with respect to protection in the provisions related to child pornography and so on. It is quite far reaching.

Mr. R. A. THORNE: Yes. Well, I am not going to deal with all exhaustively. I will just start with people and their reputations, so that, we have from you that a part of this legislation is intended to protect people and their reputations. I want clarity here.

Asides.

Mr. R. A. THORNE: I want you to understand everything I am asking and to be assured that I am not setting you up; this is no trick. We are doing this to satisfy the public that this legislation has some kind of legitimacy or validity. So let me ask you, is it possible to have a regime of law in which you seek to protect people and their reputations without also criminalising the perpetrator?

Hon. Miss M. K-A. CADDLE: Sorry, can you repeat that?

Mr. R. A. THORNE: Yes, we have agreed that a part of the purpose of the legislation is to protect people and their reputations. We have agreed on that and trust me, I am asking this to reflect public sentiment. I think part of my role is to reflect public sentiment.

Now, is it possible to protect people and their reputations without at the same time criminalising the action of the alleged perpetrator? Is it possible to have a regime of law, in which you protect a person's reputation without also criminalising the alleged perpetrator and that perpetrator being the person who has offended the person?

Hon. Miss M. K-A. CADDLE: No, it is not. Let me tell you why and I said it in my opening remarks, I do not think you had joined us yet. I think that we have enough evidence now of a level of injury; damage; hatred; associated with these kinds of crimes that supports taking these matters into the realm of criminal prosecution. I think that it is not possible to offer the level and the assuredness; the depth of protection without applying criminal prosecution.

Mr. R. A. THORNE: Thank you. That is a rather bold statement and you did mention the word hatred. Those who have studied their history, including biblical history, will tell you that hatred now is no more visceral than it was from humankind's earliest days. The difference now is that it is precisely where this legislation seeks to prevent it, in cyberspace. Humankind has not changed. Humankind has not changed. Humankind is as hateful now as he always has been. The difference is the transmission of that hatred, to use your word. What you are saying to us, that this legislation is employing the criminal law not so much to condemn changing attitudes but to condemn the transmission of that attitude to people as far away as China.

Hon. Miss M. K-A. CADDLE: I do not know what you mean by condemning the transmission of the attitude…

Asides.

Hon. Miss M. K-A. CADDLE: But it's not condemning the transmission of attitude. Let us be clear.

Mr. R. A. THORNE: The spread of the thing. We are penalising the spread of the thing; not the thing itself.

Asides.

Hon. Miss M. K-A. CADDLE*:* You asked me a question, let me answer. No. This legislation is not condemning the transmission and spread. It is condemning the result. So it is not just the fact that something has been passed or sent. It is that it has been passed or sent with the intention to do harm and that that harm has been done. That is what we are criminalising.

Mr. R. A. THORNE: This legislation, if it becomes law, would be called the Cybercrime Act.

Hon. Miss M. K-A. CADDLE: The Cybercrime Bill, yes.

Mr. R. A. THORNE: So that, the mischief that we are protecting against, which all legislation seeks to do, is that ability of the internet to spread mischief instantly and far and wide, in other words in cyberspace…. You stopping me, Mr. Chairman? How many questions do I have?

Mr. CHAIRMAN: No, but hold on.

Mr. R. A. THORNE: How many more questions do I have?

Mr. CHAIRMAN: Hold a bit. Hold a bit. The Minister has answered, saying that in her opinion.

Mr. R. A. THORNE: Yes. Oh, you are answering for the Minister.

Mr. CHAIRMAN: No. No. As I said, she said that it is her belief that you have to have a criminal penalty to….

Mr. R. A. THORNE: Yes, and I am responding to that.

Mr. CHAIRMAN: Right and you did say that you are not making a speech. Remember, we

brought her here to engage and then, to ask questions. So you could move on to the question.

Mr. R. A. THORNE: So, you do not wish her to answer the question?

Mr. CHAIRMAN: No. Move on to the question. Do not make the speech.

Mr. R. A. THORNE: No. I am not making a speech.

Mr. CHAIRMAN: Because I am sure there are other Members who also want to engage. I certainly want to as well.

Mr. R. A. THORNE: The Minister is the last of our guests today. Yes. Now, Minister, I was asking this question. I was asking, whether the legislation intends to prevent the mischief of quick spread of abuse through cyberspace. Is that a part of the mischief? Is it not a part of the mischief that this legislation seeks to prevent? That misinformation, hatred and offensive statements can travel quickly across borders.

Hon. Miss M. K-A. CADDLE: Right. It is a consideration of the legislation. The reason that the legislation is framed in this way is that, these communications do, by their definition, go quickly. It is a consideration of the legislation.

Mr. R. A. THORNE: Indeed.

Hon. Miss M. K-A. CADDLE: It is not meant to address the speed at which the communication goes. Legislation cannot do that.

Mr. R. A. THORNE: I see. Now, it is called cybercrime; the Cybercrime Bill and I take it that cybercrime derives from cyberspace. Correct?

Hon. Miss M. K-A. CADDLE: Yes.

Mr. R. A. THORNE: Yes. The phenomenon of cyberspace; a place that is borderless. Correct?

Hon. Miss M. K-A. CADDLE: Correct.

Mr. R. A. THORNE: Yes. Sorry. So that, I was asking you, whether this legislation does not seek to control expressions. I am going to use your word; expressions of hatred or offence across cyberspace.

Hon. Miss M. K-A. CADDLE: The legislation seeks to address the harm that is often caused when a person

with intent and without authorization, cause certain communication to be shared; cause certain data to be compromised and cause certain systems to be accessed. That is what the legislation seeks to do.

Mr. R. A. THORNE: We have all that but I am on the question and I am on this deliberately. I am on the question of offence against individuals and their reputations. I have not gone to data. In fact, I am not going to go to data and the infringement of data. I am on the issue of the offence to persons and their reputations to which they are entitled and I am asking you, if this legislation does not seek to protect persons and reputations because it is possible and easy to commit the offense across cyberspace; a place that is borderless? Is that not one of the primary intents of this legislation?

To protect reputations where the propagation can be committed in cyberspace and reaches anybody any part of the world? Do not answer, Senator. It is not your question.

Hon. Miss M. K-A. CADDLE: I do not know how many different ways I can answer the question.

Mr. R. A. THORNE: Do not look at him.

Hon. Miss M. K-A. CADDLE: No. I can look anywhere I want, with all due respect, Honourable Member.

Mr. R. A. THORNE: I know but he cannot help you.

Hon. Miss M. K-A. CADDLE: But, he does not need to help me; that is the thing.

Mr. R. A. THORNE: He wants to and I am telling him, mind his own business.

Hon. Miss M. K-A. CADDLE: So let us focus.

Mr. R. A. THORNE: Yes.

Hon. Miss M. K-A. CADDLE: Right. I feel like I have answered this several times.

Mr. R. A. THORNE: Okay. If you have answered it already, then leave it. Leave it. Good. You uttered a word that caught my attention. You uttered the word

"hatred". Okay and that caught my attention and I responded by suggesting to you that hatred now is no more visceral in the bosom of humankind than it always has been. That was my response and my follow up question to that. In fact, I would ask, do you agree with that? That hatred is now no more visceral than it always has been? But you mentioned hatred. You introduced it into the dialogue.

Hon. Miss M. K-A. CADDLE: It seems to have sent you off on a complete tangent.

Mr. R. A. THORNE: Yes, you have because I will come next to who determines the punishment for this hatred?

Hon. Miss M. K-A. CADDLE: Well, I would encourage you to focus on the provisions that are expressed in the Bill.

Mr. R. A. THORNE: Yes.

Hon. Miss M. K-A. CADDLE: Not to get sidetracked by my language here today.

Mr. R. A. THORNE: I am not sidetracked. You are the parent. You began by boasting that you are the parent. So, let us hear what the parent thinks of her legislation.

Hon. Miss M. K-A. CADDLE: First of all, I boasted of nothing; that was your characterisation.

Mr. R. A. THORNE: Which you accepted. Right.

Hon. Miss M. K-A. CADDLE: So, you framed me as the parent. This is….

Mr. R. A. THORNE: You did not reject it.

Hon. Miss M. K-A. CADDLE: This legislation is, by the time you have finished with your work; it will be the result not just of the Government of Barbados considerations but also the people of Barbados' own input and reflection. So, that is the first thing. What I am saying to you is, I would encourage us to focus on the language that is reflected in the legislation.

Mr. R. A. THORNE: Right. If you come to defend it, you are deemed to be the person influencing the meaning and the intent of the legislation. When the courts pore over this, they always ask the question, what did Parliament intend? Here we have the parent of the legislation; the privilege of hearing the parent of the legislation and this parent can tell us what this Parliament intends.

Mr. CHAIRMAN: Honourable Member, I think the Minister has answered that. I do not want us to go over.

Mr. R. A. THORNE: Yes, and I am on to the next question. She has answered that question. There is nothing to protect here.

Mr. CHAIRMAN: Next question.

Mr. R. A. THORNE: I am doing this in the interest of proper understanding as to the intent of Parliament. Now, I think you told us and I am going to remind you of this before I move on to the question that follows. You told us that it is not possible to protect reputations without also criminalising the perpetrator. You said that.

Hon. Miss M. K-A. CADDLE: I answered you very specifically. I said that given the level of injury, damage and so on, that can often obtain in these circumstances. You are the one who raised the issue of legislation being fit for the society. I am saying that given the level of injury and damage that we see in these cases, it in my estimation, causes these matters to rise to the level of criminality.

Mr. R. A. THORNE: Precisely, that is a long way of saying the same thing. That the possible injury is so severe that the civil law does not offer an adequate sanction. Is that what you are saying, Minister?

Hon. Miss M. K-A. CADDLE: I also offered another ….

Mr. R. A. THORNE: No. I am asking if that is what you are saying.

Hon. Miss M. K-A. CADDLE: Yes. But I am saying I also….

Mr. R. A. THORNE: Let us be clear on this. Let us be clear; let us not argue. You are saying to this country that the possible injury is so severe that the civil law does not offer an adequate sanction. Is that your position?

Hon. Miss M. K-A. CADDLE: I also offered….

Mr. R. A. THORNE: No. That is the question.

Hon. Miss M. K-A. CADDLE: This is not a court of law. But I am answering.

Mr. R. A. THORNE: No.

Mr. CHAIRMAN: Honourable Member.

Hon. Miss M. K-A. CADDLE: This is not a court of law and I answer it how I see fit.

Mr. CHAIRMAN: Let the Minister answer.

Mr. R. A. THORNE: Alright. I have it on the record, then. I was giving you the opportunity to say, yes or no. If I were you, I would have said no.

Hon. Miss M. K-A. CADDLE: But, you are not me, thankfully. So, you continue.

Mr. R. A. THORNE: I am equally grateful. Now, I am saying it is now your evidence before this Committee that you consider that it is not possible to use the civil law. Let me put it differently. You are saying that the civil law does not offer adequate sanction against the injury contemplated by this legislation. That is what you have said. Now, this legislation goes farther than the civil law and offers the sanction of imprisonment. Correct?

Hon. Miss M. K-A. CADDLE: Yes.

Mr. R. A. THORNE: Good. Are you aware that the civil law offers sanctions which are capable of ruining a person financially which is, I mean there is hardly any greater ruin than that. Are you aware that the civil law offers sanctions which can ruin a person financially that he can lose everything he has?

Hon. Miss M. K-A. CADDLE: Let me repeat the other qualifications that I offered again; I am not sure if you were with us at the time to support why we believe; these matters need to rise to the level of criminality. I mean as you should be aware there is criminal liable existing in law already.

Mr. R. A. THORNE: Which this proposes to abolish.

Hon. Miss M. K-A. CADDLE: Right, so I am saying it is not foreign to our sensibilities to have the notion of criminal liability and I would not want anyone listening to this conversation to suggest that, bringing this to the level of criminal proceedings is new. It is simply taking the notion of criminal liability; preserving it in this law but then allowing for defences at 19(5) that preserve a person's freedom of speech. Let us not suggest that bringing these matters to the level of criminal prosecution is new.

I also offered that one (1) of the reasons I believe that we must use the parts of the law available to us, is that civil proceedings require resources; require names. I cannot tell you; I grew up in a village in Haggatt Hall and it is not to say, you talk about how hatred has existed forever.

It is not to say that people have not been aggrieved; poor people have not been aggrieved before but if you are a poor person who is aggrieved by something someone has said about you; you are not able to pursue that person to get any restitution in civil proceedings. Why? Because I cannot afford a lawyer. I cannot take the time from work or the daycare to show up in court all the time. There is an extent to which, we as the State have to stand in the breach for those people who you and I represent Honorable Member; who cannot so do for themselves.

Mr. R. A. THORNE: Okay. What we glean from what you are now saying and I am grateful, is that this legislation assists with a criminal sanction for the sake of alleviating…

Asides.

Mr. R. A. THORNE: Do not worry about them. They are doing it for who they are doing it for. I am doing this for the people, so please.

Mr. CHAIRMAN: Honourable Member**, the Minister has spoken** very clearly and she was emphatic in her answers. You may disagree…

Mr. R. A. THORNE: I am not disagreeing with anything; I am asking questions.

Mr. CHAIRMAN: It is no use trying to get more out of her. She has spoken to clarity. No but hold on…

Mr. R. A. THORNE: This is the Minister who is responsible for the legislation and the people of Barbados are entitled to hear what is the mind of the Minister who is responsible for this legislation**.**

Mr. CHAIRMAN: I know but she has spoken with clarity but you are not going to get more by just repeating the same question.

Mr. R. A. THORNE: How do you know that, Mr. Chairman? Every question I asked, the Minister has answered. Every question and I have another question to ask.

Asides.

Mr. R. A. THORNE: No. This is a different question.

Mr. CHAIRMAN: Not on what she has already responded. Okay so let us hear the different question.

Mr. R. A. THORNE: Minister, based on what you have just said, that the poor man cannot afford to pursue the civil sanction; that is the last point of departure and I am asking based on that. Minister, are you saying, that this legislation, in the form of its criminal sanction compensates for a poor man who does not have the resources to pursue civil sanctions? Is that what you are saying?

Hon. Miss M. K-A. CADDLE: What you are asking me is a particular characterisation of something that I have just made very clear about.

Mr. R. A. THORNE: No. You just gave the instance of a poor man being unable to pursue a civil sanction. You said in more words than that but I am summarising. You said, *"a poor man does not have the resources to pursue the civil sanction*." There is time he may be at work and he needs money for lawyers; that kind of thing. I asked you as parent of the legislation, is the criminal sanction a compensation for the poor man who may not be able to pursue the civil sanction?

Hon. Ms. M. K-A. CADDLE: No.

Mr. R. A. THORNE: Good. Excellent answer.

Senator G. P. B. NICHOLLS: Mr. Chairman, can some of us; the others be able to ask questions?

Mr. R. A. THORNE: You mean during my questions?

Senator G. P. B. NICHOLLS: No. I just want to know, because the Minister had indicated that she had somewhere else to go. We also are Members of the Committee.

Mr. CHAIRMAN: Honourable Member, I am going to ask you to wrap up.

Mr. R. A. THORNE: Yes, I will wrap you. I am sorry. I did not know that the Minister and Senator Nicholls had to go somewhere. I am sorry about that.

Senator G. P. B. NICHOLLS: I do not have to go anywhere but I would also like to ask some questions to the Minister.

Mr. CHAIRMAN: We have asked the Honourable Member to wrap up.

Mr. R. A. THORNE: Yes, I will wrap up. I appreciate your last answer that one (1) is not done as a compensation for the other but you did say it. Now the question of jurisdiction, perhaps I should not ask that. I probably should have asked Sir David; the question of jurisdiction. Do you contemplate Minister that this legislation will be able to capture persons who commit the offence within the USA or England or Canada. Let us go for those three (3) countries. Do you contemplate that the legislation will be able to capture persons

who commit the offences in this Act within Canada, USA and England?

Hon. Miss M. K-A. CADDLE: So I am pausing to consider your framing of the question to make sure I respond.

Mr. R. A. THORNE: Well they did not want me to ask it so I can withdraw it? Then you would not have to consider it.

Hon. Miss M. K-A. CADDLE: Well you have posed it, so let me answer it. Do I consider that this legislation will be able to capture persons? Do you mean…

Mr. R. A. THORNE: Offenders in Canada, USA and England.

Hon. Miss M. K-A. CADDLE: Right and you use the word capture so I need to make sure that I am understanding you correctly.

Mr. R. A. THORNE: That the police here would be able to charge people who commit these offences under this legislation in Canada, USA and England.

Hon. Miss M. K-A. CADDLE: Yes, in other jurisdictions with whom we have agreements related to Mutual Assistance in Criminal Matters.

Mr. R. A. THORNE: Right and you have told us that the USA had signed Budapest. Canada has signed as well?

Hon. Miss M. K-A. CADDLE: The UK has signed as well.

Mr. R. A. THORNE: Yes, we know the UK has signed. I am asking about Canada because this is a premise I am now going to make to the people of Barbados; through you.

Hon. Miss M. K-A. CADDLE: Canada is party to the Budapest Convention.

Mr. R. A. THORNE: Precisely, so that it is intended Minister that this legislation will cause the prosecution of persons who commit these offences in those three (3) countries.

Hon. Miss M. K-A. CADDLE: No. It is not accurate to say that it is intended that this legislation will cause the prosecution of persons and I think your language is very loaded. Let me put it this way, this legislation and the Mutual Assistance in Criminal Matters Bill, once it passes, allows us to be able to pursue the gathering of evidence and the preservation of data in jurisdictions outside of Barbados, as applicable.

Mr. CHAIRMAN: Honourable Member, you have had a long run and we have to be fair.

Asides

Mr. R. A. THORNE: Yes but please allow me to wrap up. Just one (1) further sentence and to say to you, that Section Three (3) of the Act says that:

"This Act applies to an act done or an omission made

(a) in Barbados,

(b) on a ship or aircraft registered in Barbados; or

(c) by a national of Barbados outside the territory of Barbados, if the person's conduct would also constitute an offence under the law of a country where the offence was committed."

That is a matter, a legal question of jurisdiction; I will not disturb the Minister with that, but you (Mr. Chairman), as a lawyer, I am saying that to you so that you will understand the question of jurisdiction and that this legislation is intended to capture persons who commit the offence outside of Barbados, including Canada; including the United States; including Britain. I am obliged to you.

Hon. Miss M. K-A. CADDLE: Let me just react to that.

Mr. R. A. THORNE: Yes, please!

Hon. Miss M. K-A. CADDLE: So by definition cybercrime does not have any borders.

Mr. R. A. THORNE: Yes!

Hon. Miss M. K-A. CADDLE: So, it is possible to sit in Romania; in Senegal; in Malta; in Canada; in the United States and commit an attack on the systems - the critical data and

infrastructural systems that Barbadians need to survive.

It is possible to sit anywhere in the world and cause a Queen Elizabeth Hospital (QEH); a polyclinic; a Flow; a Barbados Light and Power to absolutely shut down for days. I do not have to be here to do it. To the extent that I do not have to be in Barbados to do it; there has to be a way for any State to pursue these criminal activities, that can debilitate its government and its people wherever these offences are taking place. Barbados is not the only country that recognises that.

Mr. R. A. THORNE: Precisely and that question of jurisdiction extends to people's rights and reputations. Thank you for the answer. That in relation to people's reputations, the offences can be committed any part of the world. Thank you, Sir.

Mr. CHAIRMAN: Okay. Senator Nicholls.

Senator G. P. B NICHOLLS: Thank you, Mr. Chairman. I am not going to be emotive at all, nor lob any insults across here. Now I want to deal with some of the points that I thought came from your presentation, Minister. I thank you and I believe the country thanks you for speaking again with such clarity on this Bill.

The Bill is about cybercrime, Minister, not cyber security; not compensating people for injuries suffered as a result of any infringements to their rights in cyberspace or so forth. I believe one of the comments or the context from which Mr. Thorne spoke, was about cybercrime and cyber offences and criminalising the offender and if this could be achieved by way of a civil redress, by way of civil law. What was your response to that? I do not think he allowed you to finish your answer. Can this be addressed by civil law or this is something altogether different, cybercrime? That is my first question.

Hon. Miss M. K-A. CADDLE: I do not think that these matters can be addressed in the realm of civil law. I think first of all, that what the world has been doing, is setting up what is essentially a criminal framework for these matters. And the only way it works is if we, as States across the world, jointly consider applicable, criminal prosecution in these matters. For example, one (1) of the things that cause people to receive no justice for offences against them, was the fact that we did not have this cross-border jurisdiction in civil matters, so that, those who tried to bring action against people who may have been in; I should not say, Serbia but Luxembourg or Croatia or the United States; those who tried to bring civil action, were not able to proceed because there was nothing that allowed them to reach across those borders, notwithstanding that the crime was borderless; to be able to pursue that.

For many reasons; for the reasons that I have already outlined because of the fact that civil pursuit did not allow you to go across borders and gather evidence from other jurisdictions; it simply is not possible to address these matters in that realm.

Senator G. P. B. NICHOLLS: Thanks, Minister. My research is suggesting that whereas cybercrime costs the international community about six trillion dollars (US$6,000,000,000,000), three (3) years ago; it is likely to cost in excess of US $20 trillion (US$20,000,000,000,000) by next year. So, this is not something to be trifling with.

You were asked about Guyana and an attempt was made to distance or to make some distinction between Barbados and Guyana in terms of the social and political setting. I looked at the Guyana Act. Guyana has misuse of devices; computer systems and access codes; critical information infrastructure systems; computer related forgery and fraud; child pornography; child grooming; online sexual abuse; cyberbullying; cyberterrorism. These are the things that are mentioned in our legislation and in theirs.

Guyana, between Sections three (3) and 24 of their Act, lists a number of cyber offences; Jamaica, a similar thing. Do you think that things like child pornography; child grooming; cyberbullying; cyberterrorism; malicious communications. Do these have anything to do with the social or political reality of the countries that we are dealing with? So as to justify changing the legislation based on the political culture.

Hon. Miss M. K-A. CADDLE: Look, I think that there is a reason that we see legislation that looks very similar across jurisdictions and especially jurisdictions in the region. I will confess that I did not gather the meaning of the

line of questioning; the related line of questioning earlier but I will say a few things: One (1) is the provisions that you just outlined that are common to the two (2) pieces of legislation are common to the two (2) countries and they are common to many countries around the world. But not only that, let us understand the importance of contagion and cross-border transmission. It really means that this notion of a society; a physical society on the ground, that is separate from an online society, is a fallacy.

There is a culture; there is an experience that our children and women and other groups of people who present particular vulnerabilities, who may present particular vulnerabilities in that sector experience, is not mirrored in Broad Street or in the Demerara; it is not about that. This is about the experience of living and working and having your being in an online environment. That online environment is the great equaliser for what many of us experience day to day…

I will give an example. I have a godson who is into gaming and he sits and ironically, one (1) of his best friends is in Guyana. He sits in his living room; his friend in Guyana is in his. Another friend is in Prague; a close friend of his who is a girl that he is often gaming with. These young people are sitting all over the world. Their reality and society is whatever is happening there. So, whereas they might be speaking French outside, for one, they might be speaking Spanish or there might be a fishing village outside, that is irrelevant. The fact is that there are certain vulnerabilities that attach to an online environment. There are certain realities and are certain risks that equalise this all across countries and cultures.

Senator G. P. B. NICHOLLS: Thank you, Minister. Looking here at the Guyana Act at Section 19 and I am sure you may not have this but it says here, *"Using a computer system to coerce, harass, intimidate, humiliate, et cetera, a person"* seems very similar to our Malicious Communication Offence. May I also take the time to remind that we had Malicious Communication as an offence, under the Computer Misuse Act of 2005 and it is almost empirical material, what is in the Bill. It is why it is surprising to me that it is now so alarming to the public.

Jamaica, who is also implementing this legislation, also has Malicious Communication almost in similar terms. A lot of some of the public criticism is that this provision was being placed here to silence criticism, particularly of the Government and criticism of politicians and so forth. You offered up today a number of suggestions to change some wording and stuff within Section 19 which is the same Malicious Communication. I just wanted you to expand a bit on the context of that.

Hon. Ms. M. K.-A. CADDLE: Yes. First of all, I think I prefaced my proposed amendments by saying that we took particular care in the defences at the Clause that relates to Malicious Communication; Clause 19. We took particular care to, in fact, preserve freedom of expression through the defences that are set out at Clause 19(5).

We understood that we were bringing the idea of criminal libel into this legislation from the Defamation Act. We wanted to make sure that the defences of truth, comment, triviality and privilege, whether absolute or qualified, provided for under that Defamation Act will also extend here. So that, if what is being said is true and the other defences represented there, that is a defence here.

I think it is also important to reiterate what Clause 19(1) says. It states, *"A person who intentionally or recklessly uses a computer system".* Intentionally or recklessly. At Clause 19(3) it states, *"a person who intentionally uses a computer system"*. So again, there must obtain the will; the intentionality to do harm through the actions.

Let me come to your question in terms of the amendments that are proposed and why they are being proposed. As I mentioned, I am offering and saying offering for your consideration. The truth is that we have in the Bill, *"a person who intentionally uses a computer system to disseminate any image or words, not caring whether they are true or false".*

To the extent that the mischief is in the falsehood. Our thinking is to dispense with the burden; the provision or the consideration of truth and to focus on the consideration of falsehood. I think that that perhaps may put at ease those who

feel that, notwithstanding that there must be intentionality; notwithstanding that there are defences; who still feel that this legislation creates some discomfort when it comes to the issue of freedom of speech.

We think that because the mischief is annoying or not caring whether something is false, so in other words, you consider that this thing has a good likelihood of being incorrect, untrue, false and you persist intentionally with its dissemination. That was one (1) of the considerations there. I think the other amendment suggested relate to Clause 20; Cyberbullying.

Senator G. P. B. NICHOLLS: Just one (1) question in two (2) parts for me, Mr. Chairman. Is there any scope for any compensation or restitutory orders being made by the magistrate? You did make reference to the fact that the standard of proof is beyond a reasonable doubt which is higher than on the balance of probabilities, which is, by the way, the standard in a civil case. if the standard is higher for the criminal case, is it within your contemplation, in the future, that some guidance

could be given to allow the courts either by way of legislation or by orders, for guidance. I know there is provision in the Bill for guidance but I am talking about giving guidance on these amounts.

Mr. CHAIRMAN: Are you sure you want to ask Minister Caddle that? Minister Caddle is not a lawyer.

Hon. Miss M. K-A. CADDLE: With all due respect, Mr. Chairman, we are all legislators in here.

Mr. CHAIRMAN: Under the 1997…. Oh, I cannot remember the exact name. Penal…Penal…; That would have been passed here in Parliament…

Senator G. P. B. NICHOLLS: Penal System Reform Act.

Mr. CHAIRMAN: Right. Restorative justice is always an option.

Senator G. P. B. NICHOLLS: Yes, but there is a provision in this Act for compensation. I am not asking about whether we can because the jurisdiction to grant compensation is here. I do believe that this legislation can only work in certain parts, if there is guidance given and regulations issued into how certain things are to be operated and eventualised. So, I am asking whether or not that is within the scope. The Ministry will have to issue such guidance or some Ministry or some authority of the Government. So, that is why I am asking the question, Mr. Chairman.

It is either not contemplating it now or because you do not want situation where then it is left to the magistrate in District 'C' or the magistrate in District 'A' to determine compensation or what guides compensation in relation to these matters. This legislation is *sui generis*. This is not anything of a similar class that exists right now. Orders for compensation which is now creating this recoverable civil debt against a person who has made a malicious communication via some internet device or computer device. That is the question I wanted to have some clarity on.

Hon. Miss M. K-A. CADDLE: You are asking if there is scope which is a pretty low bar. I would say there is scope. I take your point and your meaning. It is something that I have also reflected on, that there are scenarios of criminal prosecution in which restitution, alongside the criminal penalty, perhaps serve the offended party best or perhaps serve best so I would not want to say that it is beyond the scope.

Senator G. P. B. NICHOLLS: Section 30 does give you the power to make regulations which comes after Section 29 which is the power to Order Compensation.

Hon. Miss M. K-A. CADDLE: Yes, and I think that in that Section it makes it possible. I would not want to say this is something to which we would go immediately but as in other areas of legislation; yes, I think it within the scope and I do see the value that could obtain in the future of such cases.

Let me do clarify that I want us to be clear with our purpose in this legislation which is that, there is an extent to which there is public damage as well that is caused by these offences and that is another reason why I believe that civil pursuit

does not serve completely. When you have a case, scenario ore situation where attacks made or harm done in this realm continue unchecked. That contributes to a certain sense of disorder and absence of governance and so I say that to suggest that a part from the injury to the person, there is an injury and damage to the society when these things are allowed to stand.

I really encourage Barbadians not to be sidetracked by the over-emphasis of a particular area and be reminded that this legislation is one (1) about protecting people's information. It is about protecting children in an online environment. It is about making it so that what happened to those two (2) women in the context of the US election where they lost their reputations; their safety; their work; their homes, that it is not something that takes over. That is not something that is done of a matter of course.

That people feel that there are not consequences for the utterances that they make. There are consequences. There have always been consequences for the ways in which we speak about people. The ways in which we gain access. The truth is that a lot of what is covered in this legislation; it is akin to gaining unlawful access to a person's home; being able to break into the systems of the State, where there is information related to an individual. That is what Barbadians are insisting on. They are insisting on the kind of Data Protection that this legislation allows and that is why I said at the outset, that pausing this Bill, to have these conversations allow us to reflect on what we want.

Bajans have said very clearly that they want this kind of protection. We all now I daresay in this room, people whose lives who have very adversely affected in Barbados, by the kinds of actions that this legislation criminalises. I do want us to step back and consider this thing in its entirety; to be able to understand that this is primarily about protecting individuals who can ill afford to protect themselves.

Most of us in here do not need the State to represent us if someone says something about us that cannot be supported or that does damage to us. I keep hearing thrown around this room this afternoon, this notion that I am speaking for the people outside. This legislation is speaking for the people outside. This legislation is about making sure that even in cases where a person does not have the wherewithal, the resources to defend against these kinds of attacks that the State is going to step in on their behalf and so, I do believe that we have listened. I certainly have in my own reflection and what you have heard today is a result of my own reflection to what might have given people some pause but I think that this country will be the better for passing this legislation which as you have highlighted Senator Nicholls; really is a revised and renewed version of legislation that has existed before or has existed in other places.

Senator G. P. B. NICHOLLS: Just to leave you with this one (1) comment because the impression might be conveyed that you are the parent of this legislation but you are actually the person who piloted the Bill and what you say about this Bill, whether in here or in Parliament will not in any way affect how a court interprets legislation and you do not like anyone to interrupt you. You should have some manners.

Mr. CHAIRMAN: Honourable Members. Honourable Leader of the Opposition, please. Senator Nicholls please proceed.

Senator G. P. B. NICHOLLS: He is now waking up.

Mr. CHAIRMAN: Senator Nicholls proceed to ask the question. Senator Nicholls proceed to ask what you are asking.

Asides

Senator G. P. B. NICHOLLS: I just wanted to be very clear and for the public, who is watching and yourself that whatever you say is not going to be a basis in which the court interprets the meaning of the legislation. When…

Mr. CHAIRMAN: Honourable Leader of the Opposition.

Asides.

Mr. CHAIRMAN: Honourable Leader of the Opposition you had a lot of length. In fact, you yourself said that you were making speeches; so Honourable Senator please proceed.

Senator G. P. B. NICHOLLS: Thank you, Mr. Chairman because I am proceeding to something that he is.

Mr. CHAIRMAN: Honourable Leader, you are out of order. Honourable Senator please ask the question.

Senator G. P. B. NICHOLLS: Sir, he cannot help.

Mr. CHAIRMAN: But do not mind that. Ask the question.

Senator G. P. B. NICHOLLS: When we hear about the court will interpret as the Honourable Leader of the Opposition has said in here, the Honourable Leader of the Opposition has indicated.

Asides.

Mr. CHAIRMAN: Honourable Leader of the Opposition you are out of order. Senator Nicholls, just ask the question please.

Senator G. P. B. NICHOLLS: I am glad that the public is watching what happens; when you are the only person in a place that has any sense everybody will believe you but now he is getting a little fight back on his words. Thank you. Mr. Chairman, the Honourable Leader of the Opposition has suggested.

Asides.

Mr. CHAIRMAN: Do not mind the Honourable Leader of the Opposition.

Senator G. P. B. NICHOLLS: I am not minding him; I am speaking. The Honourable Leader of the Opposition suggested to the Minister that because she was the parent of the Bill, what she had in fact says in here goes on the record that the Courts will interpret. I am responding to that comment. He does not like what I have to say but I have the right to say it and I also believe the public have the right not to be misled by Senior Members of the Bar who know better, right?

Any interpretation of this Bill when it is passed, the first thing the courts will do is look at the language of the Bill. The courts will adopt what they appropriately call a Purposive Interpretation.

Mr. R. A. THORNE: But how is this relevant, with all due respect to the Minister's purpose here this evening. What the courts may or may not……

Asides.

Mr. CHAIRMAN: Honourable Leader of the Opposition, you had your turn…

Asides.

Senator G. P. B. NICHOLLS: The Honourable Leader of the Opposition misled the public when he suggested that the Minister because she was the parent of the Bill, the answers to his questions, in here, would be the basis upon which the court would interpret the legislation.

Asides.

Senator G. P. B NICHOLLS: I made my notes then and I am making the point that this Committee should not accept that because that is nonsense on stilts, that the court will interpret the Minister's answers to his questions, as the basis of how the legislation should be interpreted.

Asides.

Mr. CHAIRMAN*:* Okay, Honourable Members, we are going to settle down in here now. Honourable Senator, you have made your point and you are correct in my opinion. Is there another point?

Senator G. P. B NICHOLLS: No, Mr. Chairman. I just wanted to make that clear for the record because I did not want the Minister or the public to go away with the impression…

Mr. CHAIRMAN: I do not think that a reasonable public would have taken what the Opposition leader said.

Asides.

Mr CHAIRMAN*:* Honourable Members, please. This will stop now. I know this has been a long day. Senator Nicholls; Member of Parliament, please!

Asides.

Mr. CHAIRMAN: I just wanted to say a few things to draw your attention to; a few sections, Honourable Minister. The first thing is that the Budapest Convention. Honourable Members! Come on! You all are members of the legislature; we have to set a better example. There is no cross-talk in here now. Well, we stop!

The Budapest Convention is a European Convention. Barbados is not a member of the European Union (EU) or the Council of Europe and therefore it is not, for example, a situation like a UN Convention where Barbados is a member of the United Nations and the Council of Europe has said that any person who wants to sign on to the Budapest Convention must pass cybercrime legislation before signing on. So, the point that the Honourable Leader of the Opposition was trying to make, as…

Asides.

Mr. R. A. THORNE: I was not trying to make a point; I was asking questions…

Asides.

Mr. CHAIRMAN*:* The second issue is that the Computer Misuse Act has had criminal penalties for almost two (2) decades, this is not the first time that issues relating to malicious communication, for example, will be subject to criminal penalties. The Act is not bringing anything new in that respect; it is expanding on the Computer Misuse Act, which has been part of the law of Barbados for almost two (2) decades.

The third thing is that we focused on Guyana. Guyana's legislation was in 2018; Jamaica's was before that. Jamaica had similar cybercrime legislation since 2015 and Jamaica is not polarised by the racial divisions that the Hnourable Leader of the Opposition was seeking to portray in the case of Guyana.

Mr. R. A. THORNE: I was not seeking to portray anything; I was asking questions.

Mr. CHAIRMAN: We understand that and I am helping to give clarification here.

Mr. R. A. THORNE: We came here to pursue whether there is any change needed to be made to the legislation and the Honourable Minister came here today and suggested that there are changes that need to be made to the Bill. Please record what the Honourable Minister said.

Mr. CHAIRMAN: Yes, we are aware. I am putting on record that Jamaica as well, has similar legislation even before Guyana and Jamaica, I do not think anyone would wish to suggest, is polarised by race.

Mr. R. A. THORNE: But Mr. Chairman is this part of your duty?

Mr. CHAIRMAN: Yes.

Mr. R. A. THORNE: it is? If it is, I will keep quiet.

Mr. CHAIRMAN: I hope so.

Asides.

Mr. CHAIRMAN: Yes, you had your chance for a long time. So, Honourable Minister, I am going to just ask you to look at some sections of the Bill as drafted. Section eight (8), Illegal Interception of Data, where the fine is $100,000, maximum fine, as we have indicated, over and over; imprisonment, 10 years or both. I am just wondering if you, on reflection, as you said, you have done and I thank you for, you know, the amendments you have come here and proposed today. If, on reflection, you would think that this is a bit harsh? Sir David felt it was and may be that those could be adjusted, as the others are, the $70,000; imprisonment or seven (7) years.

Hon. Miss M. K-A. CADDLE: Okay, just so that those listening are clear on what we are talking about. Illegal interception of data:

"A person who intentionally and without authority undertakes an act to intercept, by technical means, any non-public transmission to, from or within a computer system, including electromagnetic emissions."

I want us to understand what this is, why the penalty is higher, "*including electrical electromagnetic emissions", s*o you have not even gained access to the computer system. You are within sufficient distance to pick up emissions from a piece of equipment or a system, including electronic electromagnetic emissions from a

computer system carrying computer data, is guilty of an offence and is libel on conviction of indictment to a fine of $100,000 or imprisonment for a term of 10 years, or to both.

Why does this carry a higher penalty? Senator Nicholls quoted earlier some figures with respect to the economic loss that we have seen and that we can expect from cybercrime. In this field, interception of data and intercepting non-public data is one of those acts where we have seen the highest damage and loss.

We are talking about the act of going on website to put in the password for your bank; somebody intercepts that information that is meant to be a non-public transmission; someone gains access to your entire bank account; to your company's bank account and is able to steal resources; is able to disable a company; is able to. I mean in many jurisdictions, the penalty is even higher because of the scale of theft that it allows for electromagnetic emissions. So, just imagine.

This kind of act is often also used with respect to terrorism. You are somewhere else in the world or you are not even near the computer system and you have a device that allows you to pick up emissions from a computer system and use those to commit a crime. I explain that because I want us to understand that this is not just a question of looking at a number and saying, that is too high. There is a reason that there are higher fines associated with certain provisions in this legislation. If it is the judgment of the Committee that or if it is the recommendation of the Committee not the judgment; that a lower fine can be suggested, that is within your purview to do but I am cautioning you that it has to be indexed to or it has to be with reference to the other offences or the other fines, in terms of imprisonment because it is considered potentially a far more damaging act. I would offer that as my response.

Mr. CHAIRMAN: Thank you for that explanation. Section 11; Disclosure of Access Code. Section 11(1) and 11(2) seem to be quite similar. I was wondering if you would wish to agree that one (1) of them could be removed. Let me read. It is Clause 11 (1) is as follows:

"A person who intentionally or recklessly and without authority discloses any password, access code or any other means of gaining access to any programme or data held in a computer system is guilty of an offence and is liable on summary conviction to a fine of $25 000 or to imprisonment for a term of three (3) years or to both."

Clause 11 (2) is as follows:

"A person who intentionally or recklessly and without authority discloses any password, access code or any other means of gaining access to any programme or data held in a computer system for any unlawful gain, whether to himself or to another person, knowing that it is likely to cause unlawful damage, is guilty of an offence and is liable on conviction on indictment to a fine of $70 000 or to imprisonment for a term of seven (7) years or to both."

I know subsection (2) adds on the unlawful gain aspect and knowing it is likely to cause unlawful damage.

Hon. Ms. M. K.-A. CADDLE: I was going to tell you, Mr. Chairman, that you accused me of not being a lawyer and you cautioned Members not to address me as they would a legislator but it seems to me that I am able to pick up the finer points of these two (2) Clauses a little bit better. Let me go further.

As you have highlighted at Clause 11(2), it makes the point about unlawful gain and again, similar to the earlier Clause that I explained; the distinction being made here is the intent. So, at subsection one (1):

"A person who intentionally or recklessly and without authority discloses any password, access code, or any other means of gaining access to any programme or data held in a computer system is guilty."

So, at subsection one (1), a person intentionally or recklessly and without authority; those things in themselves, you disclose a password or access code or a means of gaining access, you have done so intentionally or recklessly and without authority may not be for any

particular purpose but you have done so. That carries a lower fine or term of imprisonment.

At subsection two (2), the unlawful gain; the intent to defraud; the intent to steal; the intent to pass those resources on across borders for all kinds of reasons and to fund certain kinds of activity, that is what imputes or that is what attaches the higher penalty.

I would not agree that they repeat themselves. I think that the distinction is being made. At subsection one (1), there is intent to pass on the code that you know you do not have authority to pass on. At subsection two (2), there is intent to pass on the code and there is further intent for unlawful gain such as, again I described having access to a bank account or being able to impersonate a person who is able to authorise certain financial transactions. I think that level of criminality goes a bit higher and that is why the two (2) are separated. Again, if you have recommendations for the level of fines, I am sure that is something that could be considered.

Mr. CHAIRMAN: Thank you for that. I am just giving you the opportunity to respond to some of the criticisms and points that were made earlier. In terms of corporations, this Bill as drafted, only seeks to penalise corporations under Section 17; Child Grooming. Section 16, I think it is, the Child Pornography and Section 18; Sexual Abuse.

While other legislation, certainly Jamaica's brings corporations under its penal provisions through penalising the director, manager, secretary or similar company officer. We are wondering why perhaps corporations were not penalised or subject to penalty throughout the Act but only for those three (3) provisions. Is there any particular specific reason?

Hon. Miss M. K-A. CADDLE: Your suggestion is that corporations should be subject to criminal penalty for what kinds of offences?

Mr. CHAIRMAN: Cyberbullying, for instance, Cyberterrorism.

Hon. Miss M. K-A. CADDLE: You are suggesting that a person who is employed by a corporation who engages in these activities should cause the corporation to also face criminal prosecution?

Mr. CHAIRMAN: Acting within the scope of their employment as agent for the corporation.

Hon. Miss M. K-A. CADDLE: Acting as an agent for the corporation would mean…. Proving that they are acting as an agent for the corporation is an interesting one (1) but acting as an agent for the corporation would mean that the corporation should also face a penalty.

I do not like to respond to matters of policy and law on the flight but I would suggest to you, I have no objection to, obviously, to considering a recommendation of this Committee that frames that. We will see how it lines up with the rest of the Bill.

Mr. CHAIRMAN: Thanks for that response. Section 19, the Intimidation. We all recognise that this is one of the most controversial sections. He intimidates and you also refer to the question of intimidation. Well, you said you would have put it a different place; the definition of it. But, under Section 19 (4), intimidate also can mean causing a person substantial, emotional distress. The question arose as to whether that aspect of intimidation; the definition of intimidation, should also be ring-fenced by the Defamation Act defences.

Hon. Ms. M. K.-A. CADDLE: You are suggesting what language, Mr. Chairman?

Mr. CHAIRMAN: That the same way how Clause 19(3) is covered by the defamation defences; should consideration not be given to causing a person's substantial, emotional distress and be ring-fenced by the defamation defences as well?

Hon. Miss M. K-A. CADDLE: You are saying that what is covered at subsection three (3), the defences should obtain equally for three (3) and four (4)?

Mr. CHAIRMAN: No, not all four (4) because to intimidate by telling someone you are going to injure them or the family or do violence to them or damage to their property or to themselves, I cannot see how defamation defence could be applicable there.

Hon. Miss M. K-A. CADDLE: Right. That is what I was going to suggest.

Mr. CHAIRMAN: But for the third thing, Clause 19(4) (a)(iii); *"causing a person substantial emotional distress"*, whether that could fall in the same category?

Hon. Miss M. K-A. CADDLE: I do not quite agree. Perhaps, this is a finer point of language but I think that the defences of truth and so on, I do not really see how they apply. Remember that three (3) is a sub-section of (a), intimidate; it is a part of the definition of intimidate and so to the extent that you are not just caught talking about, *"a person intends to use a computer system to disseminate image or words not caring rather they are false and likely to cause,"* I think we had said embarrassment is guilty of an offence. I would say to you Mr. Chairman that these definitions are very different. I am not sure that Defamation obtains at four (4) because intimidation is defined as it is defined so it.

Mr. CHAIRMAN: But it is not all one (1). It is the apprehension of *"violence or injury or substantial emotional distress."* So I was just wondering if you could take out the *"substantial emotional distress"* and put it in three (3) so it is covered by if what you are saying is true. For example, or trivial that they would be that defence.

Hon. Miss M. K-A. CADDLE: Again, if the Committee wishes to suggest a particular amendment that you think makes the legislation stronger or clearer it is something that we would consider. In my mind, definition of intimidation is so separate from what the defences are meant to apply to at three (3), that I saw them as separate but again, I am not going to sit here and accept or deny a recommendation unless it is completely at odds with the intent of the legislation, so invite the Committee to make its recommendation.

Mr. CHAIRMAN: Okay and the last one, Minister. As you are aware, some people have criticised Section 23 going forward and the issue of a "Search Warrant by a Judicial Officer" and I think, we agreed that Section 23 (1) where it says, *"The Magistrate may issue a warrant,"* should also say "The Judge" or "Magistrate" but the question has arisen as to which police officer?

Section 23 speaks towards any police officer being able to go off and apply for a search warrant from a judicial officer; whereas later on for example, Section 28 speaks towards Commissioner of Police or any other Gazetted Officer; Section 27 judge or magistrate being satisfied on an *ex parte* application by Commissioner or other Gazetted Officer.

I was just wondering if similar to Guyana, that the officer has to be at Superintendent level or above to be able to go and apply for a search warrant from a Judicial Officer on oath and I am just wondering whether you would be amenable and you cannot bind yourself. I am just addressing your mind to it; whether Section 23 should limit it to Gazetted Police Officers?

Hon. Miss M. K-A. CADDLE: What is the mischief that you consider there, Mr. Chairman?

Mr. CHAIRMAN: Well, that the Officer should have some senior rank to be able to go and apply on oath to the Judicial Officer to get a search warrant. I think the concern as I read it from some Barbadians, is that any police officer and some police officers may just do it on because they do not like you or because you did them something and I was just wondering if it may perhaps be better to limit that to more Senior police officers.

Hon. Miss M. K-A. CADDLE: I would say that I would be willing to be guided by what obtains for other kinds of warrants. Remember a computer is not a magical thing. It is just a domain in which the activity and certain procedure is taking place. I would be guided and we should all be guided by what obtains for search and seizure in other areas of legislation. I am not wedded in any particular way to this particular provision but I would encourage us to be guided by that.

What I will say is that when it comes to preservation of data and warrants regarding the preservation of data that we should not increase the level of authority because as I mentioned to the Committee earlier, a warrant for the preservation of data is really just to be able to stop the data from being destroyed and in many other jurisdictions, it does not even require judicial intervention. It does not require law enforcement intervention.

We maintained that because of our social need and circumstances but we do have a trade off

in the sense that in a way, it could defeat the purpose of preserving the data if there is too high a level of authority, such that, it takes too long remember it is just preserving. You are not harming anything and you are not changing anything. It is just to stop it from being destroyed in the hands of a third party so it is not in the hands of government or the hands of a telecommunications provider or so on, that we not increase the burden there.

We already have it and our legislation is actually the only one (1) that requires a warrant for data preservation but that wherever we should preserve it, not to use the word in two (2) contexts but we should keep the level of authority for data preservation for where it is but if you want to recommend a change in keeping with search and seizure in other legislation; there is no need to have special provisions here. The computer is just the domain; no different from a house or a public place, so that would be my only guidance.

Mr. CHAIRMAN: Thank you for that response and for your responses. Minister, we thank you for coming this afternoon to expand your thoughts as Minister responsible for this Bill; responsible for presenting it. We appreciate that you on reflection proposing yourself some amendments to it and we have now closed off the oral hearings on this. We have the written submissions and we clearly will set some timelines and when we could reflect on it and get a report back to Parliament.

Hon. Miss M. K-A. CADDLE: Thank you. Just in the final two (2) minutes, to say that this has been a very rambunctious proceeding; far more so than I expected it to be but just to give my thanks truly to the Members of this Committee. I perceive that you are passionately defending your various positions and that you have brought a certain level of rigour to the analysis and I also want to say to the people of Barbados that I feel quite privileged that this legislation has enjoyed the level of engagement; has attracted the input and the discussion.

I do not consider that what has transpired with respect to the cybercrime legislation is at odds with the democratic spirit of this country. I think it is very much aligned. I have a sense of pride in the extent to which Barbadians are willing to consider the policies and legislation that affects them and to attempt to have an informed position. I focus on informed because I think it is important that we not encourage misunderstanding willfully and that we instead lead our various; guide our various spheres of influence towards honest debate.

In that regard, I consider that some of the feedback has been useful; some of the concerns have been genuine and I am grateful to have had the opportunity to reflect on those with the Members of this Committee and I feel confident that we will emerge with effective and useful legislation to deal with these matters. So, I thank you.

Mr. CHAIRMAN: Minister, as you know, I said at the beginning here this afternoon, the Senate is going to have to deliberate on an expansion of our mandate. Let me ask you this question, what kind of timeframe are you looking at in terms of a report?

Hon. Miss M. K-A. CADDLE: You know, to the extent that these matters are national security matters; a lot of what is represented in this legislation is really the subject of a national security conversation. I am always hesitant to say too much in that regard, suffice it to say that what has motivated us to pass this legislation is upon us. What has motivated us to pass this legislation is upon us.

The risks that exist are near and present. In the region, we are aware of certain exigencies. I would say that the timeline is now. I would wish to prevail upon you, Mr. Chairman and the Committee, to allow us to have a report that would mean we can advance this legislation as soon as possible.

We have events coming up that mean that we will have the world at our shores and I really would urge us to proceed with dispatch. This again; for matters of safety and security, we have to have a maturity of political cooperation. That means that we unite to protect this country and our citizens and so I would encourage you to move with as much haste as possible. I think I have said enough for you to get my meaning.

Mr. CHAIRMAN: Okay, thank you.

(Minister Caddle leaves the Senate Chamber and the meeting resumes).

Mr. CHAIRMAN: So the issue is, as I said earlier, our mandate expires on Thursday. The Senate is meeting this Wednesday, as I understand it…

Senator G. P. B. NICHOLLS: So there are three (3) Senators here, Senator Walters and Senator Nurse and I. We do not foresee any difficulties in getting an extension for this.

Mr. CHAIRMAN: But the question is, until when? You have heard the Minister speak, obviously, in reference to the World Cup …

Senator G. P. B. NICHOLLS: Mr. Chairman, it would not be for us to say. I believe the Clerk would have to indicate to us because the writing of the report and the final deliberations and those processes have to be informed by those timelines.

Mr. CHAIRMAN: Do we ask the Senate for an extension for a particular date or the Senate leads that?

Senator G. P. B. NICHOLLS: That is informed by the Clerk. I am just saying…

Asides.

Mr. CLERK: Based on what I have just heard and taking everything into consideration; it appears as if this report not only has to be done but the debate completed by the end of this month or before the end of this month. Today is the 13 May, 2024; next Monday is a Bank Holiday - Whitsuntide.

Now, the Senate is meeting Wednesday; the Parliamentary Reform Commission (PRC), which I am Secretary to, is already behind in terms of deadlines, Thursday and Friday. So effectively, what it means is that we really have; I would say a week to have the report ready.

Asides.

Mr. CHAIRMAN*:* But obviously we have to deliberate…

Asides.

Mr. CHAIRMAN: Tomorrow is Lower House; Wednesday is Senate and you are saying Thursday and Friday is PRC. Hold on, hold on! Your staff can meet because we now obviously, we would not be deliberating in public.

Mr. CLERK: When PRC meets, the same staff that you see here; works with PRC. The same staff that would be streaming, works with PRC.

Mr. CHAIRMAN: I see in the rules that we can meet on a Saturday. Mr. Clerk, I am seeing in the rules that we can meet on Saturdays. Are we available on Saturday?

Senator G. P. B. NICHOLLS: No, Mr. Chairman.

Mr. CLERK: There is also something called a work/life balance and I am suggesting that we not meet on Saturday.

Mr. CHAIRMAN: So, Monday is a Bank Holiday. Most likely, Tuesday next week is going to be Parliament. So, when are you suggesting we can meet, Sir? It will seem as if we will meet on Wednesday. If Wednesday is the Senate?

This is what I would suggest. We have heard all of the evidence. I am assuming we have read the written submissions; over 40 as they are. We have heard the oral evidence. Can we have Members individually start working on what amendments, if any, they propose so that when we do meet, that we all come and see how far we can reach a consensus on proposed amendments? Such that, we only have to meet once to deliberate.

In the meantime, obviously Clerk of Parliament, for your staff and I know it is difficult because you have the PRC too. This is one of the problems because as we all know, I am not saying anything secret, there were big advertisements in the newspaper. What? September last year, for more staff. This is now the dilemma.

Senator G. P. B. NICHOLLS: Mr. Chairman, I think we need to come down on a date that the Committee will meet again and perhaps, leave some room for a final meeting

because I suspect that one (1) set of deliberations might not be sufficient. Next week looks to be pretty much out but when we go into….

Mr. CHAIRMAN: But, you heard what the Minister said. World Cup, as you know better than anybody else in here, is starting in just over two (2) weeks time.

Mr. CLERK: Mr. Chairman, what I would suggest is, I would say next Wednesday. The Government cannot want this work completed and this Bill before the Senate before the end of May and then also ask the Senate to meet next week Wednesday. It would mean that something would have to….

Mr. CHAIRMAN: So, you will point out to the Leader of the Government Business in the Senate.

Senator G. P. B. NICHOLLS: Thursday is still possible.

Mr. CHAIRMAN: Thursday is possible too.

Senator G. P. B. NICHOLLS: So, I am just saying that the safest day is Thursday, next week.

Mr. CHAIRMAN: Thursday and Friday as a….

Senator G. P. B. NICHOLLS: I have to travel on the Friday to go to that place where you just came from, Mr. Chairman; where Mr. Thorne likes so much.

Mr. CHAIRMAN: Where did I now come from? I did not come from Guyana. I came from Trinidad.

Senator G. P. B. NICHOLLS: They do not have cricket.

Mr. CLERK: So, Senator Nicholls you are on for Thursday?

Senator G. P. B. NICHOLLS: Thursday, next week, seems to be the safest date. I sit at the risk of not even seeing my court calendar but I would make adjustments.

Mr. CHAIRMAN: Okay, so Thursday next week. I mean, well, that is the only day because we do not know what is happening on Wednesday. Unless, I would say, on Wednesday and you would know obviously on Wednesday, whether the Senate will meet next week, Wednesday. Let us say Thursday but if the Senate is a meeting next Wednesday, then Wednesday. Alright?

We would want Members to come prepared, in other words, to have, what they would like to see amended before us, so we can have a discussion. In the meantime, as well, Parliamentary staff, that you all start formulating because I know that these reports follow a set format.

Mr. CLERK: Mr. Chairman, just before you get to the format. So, on Wednesday, we are asking Senator Nicholls as a Member of this Committee, to request an extension of the time for reporting to be no later than the end of the month? Is that the time?

Senator G. P. B. NICHOLLS: That is if we are going to be able to complete the work; so, we do not have to ask for another extension.

Mr. CLERK: No. I was just using, based on what you heard from the Minister, where the timelines are in relation to this legislation.

Mr. CHAIRMAN: Wednesday next week is what date? Today is 13 May, 2024. Right? So, Wednesday next week is 22 May, 2024.

Senator G. P. B. NICHOLLS: Mr. Chairman, let me be very frank. I understand the Minister because we are …. The fact that we do not have Cybercrime Legislation continues to keep the country at a level where we are exposed to persons who might threaten our security infrastructure and try to penetrate it because they know there is no likelihood of Barbados being able to co-operate with somebody in a jurisdiction where they are affected. So, that is why I understand the Minister says it because the threats are always ongoing.

There is somebody right now who is dealing with a phishing email or something like that right now. This is something that happens daily. Right. Anybody who has had to deal with

Caribbean Broadcasting Corporation (CBC) or the Queen Elizabeth Hospital (QEH), by way of email, would have gotten certain emails coming to their systems.

I get them all the time because you communicate with people and their system was corrupted. So, this is not something that is not urgent; it is urgent but the more important thing is for us to complete this process in a proper way. I do not think the Minister is trying to put a gun to our head by saying we need to complete it before World Cup because the security arrangements for World Cup are not necessarily contingent on this Bill passing.

I do not want to give that impression. So, if we go into early June; I speak subject to correction but if we can get our work completed, then fine. I do not think that we should put ourselves under the view that we need to complete this before World Cup because World Cup needs this to happen. That is not correct.

Mr. CLERK: So, 15 June, 2024 then? 15 June, 2024 as an extension?

Senator G. P. B. NICHOLLS: Yes because I saw the report you issued last week on the Child Justice Bill and it has 800 pages. I was trying to attempt to download it.

Mr. CHAIRMAN: A lot of it if you look at it; not much of it is deliberations because it is all the evidence that they had. The written submissions, remember, it is two (2). So, the Child Justice Bill….

SENATOR G. P. B. NICHOLLS: Mr. Chairman, I have not read it.

Mr. CHAIRMAN: No but I am telling you because I read it yesterday. The old Child Justice Bill; the new one; the old Child Protection Bill and the new one. So, it is not that much, do not mind it is 800 pages.

Senator G. P. B. NICHOLLS: I hope that when the Parliamentary Reform Commission completes its work; it needs to know that if we want to do the business of a modern Parliament, that you have to resource the Parliament and its members to do the business of Parliament.

Mr. CHAIRMAN: Yes. You mean research officers and….

Senator G. P. B. NICHOLLS: Not only research, you know because those of us who are on stipend …

Mr. CHAIRMAN: That is another matter.

Senator G. P. B. NICHOLLS: It is important work that we do. Right. But, we have had to shut down all the things we do. I am sure Members of Parliament like yourself, have things and pressing things to do. We have another meeting which started already.

Mr. CHAIRMAN: I know. It is a full-time job. Honourable Leader, what is your position?

Mr. CLERK: I just want to follow up on what Senator Nicholls is saying. Apart from stipends and those resources; one (1) of the constraints is the actual physical space to meet. Now, as you aware, this is probably the only meeting room that we have and the Senate meets here. PRC meets here.

Mr. CHAIRMAN: That is not really true because I notice the Social Committee met in the Ermie Bourne Committee Room.

Mr. CLERK: But, the Ermie Bourne Committee is not resourced for streaming.

Mr. CHAIRMAN: Right but, I mean for our deliberations now because our deliberations will not be recorded.

Mr. CLERK: No. We record the deliberations.

Mr. CHAIRMAN: They are recorded as well, too? Okay. I am scheduled to travel on 11 June, 2024 on Government Business so I would want to suggest the 08 June, 2024. I do not want to leave with this still before us. Friday, 08 June, 2024. Friday is the 07 June, 2024. Friday, 07 June, 2024 to ask the Senate. When the Senate meets is out of our control. Our remit now is to get a report. Friday, 07 June, 2024. The Senate will be asked to extend our mandate until then.

Senator G. P. B. NICHOLLS: Mr. Chairman, is it possible for; I know we did not get the minutes from the last session and today but the

Minutes that we have gotten. Not the Minutes, the transcripts for the first two (2) meetings was excellent. That made life easy and it made Sir David's presentation and such but the last two (2) sessions we would need but…

Mr. CHAIRMAN: When can we get the Minutes for last week and today?

Senator G. P. B. NICHOLLS: I am asking for something a bit different. Is there going to be someone who is going to look at the transcript and pull out the main issues for us? Amendments and reforms; where there was consensus or suggestions by Sir David; the Minister and from the various Members? Is there someone that is able to do that? I know I am not trying to put more pressure on Pedro and his staff but that would be helpful if you pull out the 10 points on which was discussion on amendment.

Mr. CHAIRMAN: How many transcripts have we had so far? Just one (1)?

Senator G. P. B. NICHOLLS: We have two (2). The first two (2) meetings.

Mr. CHAIRMAN: I just have one (1). Monday, 8of April.

Ms. Suzanne HAMBLIN: No, two transcripts were completed. It is only the last meeting that is not completed as yet.

Mr. CHAIRMAN: So give me the other one. You have the one after Monday, 08 May, 2024.

Mr. CLERK: What I can get to you because we have been using Artificial Intelligence (AI).

Senator G. P. B. NICHOLLS: AI can pull out amendments; not suggestions.

Mr. CLERK: What I can get for you by the end of this week is an unedited version of all the transcripts of the Meetings that this had so far.

Mr. CHAIRMAN: Senator Nicholls says he has one (2) for the second. So you all have that?

Senator G. P. B. NICHOLLS: Sir David's one (1) was given to us. We have met four (4) times?

Mr. CHAIRMAN: Sir David's? I only have this one (1). Get one (1) for me.

Mr. CLERK: What I am saying, Mr. Chairman that all the Members have it because it was emailed.

Mr. CHAIRMAN: But what I am saying is that I do not have it so just get it for me. I understand but I just do not have it so what I am asking the staff to do is to just give me it here because I definitely do not have the one (1) with Sir David. You would now have to print it out for me? Pardon? Okay. I will stay because I still have to look and sign these Minutes here so just print it out and give it me.

Senator G. P. B. NICHOLLS: So Pedro, your AI can also pull out any discussions on possible amendments or…

Mr. CLERK: I will ask the Information Technology (IT) guy. Once he puts it, it should be able to pull that but the way we have been. It will be unedited. You can have that transcript ready half an hour after a meeting so as I said, by the end of this week for sure, you should be able to have all of those. The edited transcripts now wait on the Hansard.

ADJOURNMENT

Mr. CHAIRMAN: Okay, so unless there is anything further we are going to move to adjourn to Thursday, 23 May, 2024. If the Senate is not meeting next week Wednesday, for us to meet next week Wednesday, 22 May, 2024.

The meeting was subsequently adjourned to Thursday, May, 23, 2024 at 10:00 a.m.

5th MEETING
JOINT SELECT COMMITTEE (STANDING)
ON
GOVERNANCE AND POLICY MATTERS
ON THE
CYBERCRIME BILL, 2024
AND THE
MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024

Thursday May 23rd, 2024

PRESENT:

Mr. Edmund G. HINKSON, S.C., MP, LL.B. (Hons.), L.E.C., LL.M. **(Chairman)**
Mr. Peter R. PHILLIPS, MP
Mr. Ralph A. THORNE, K.C., LL.B., L.E.C., Dip. Theology
Senator The Hon. Lindell E. NURSE, F.C.A, F.C.C.A., R.C.S. (ENT)
Senator Gregory P. B. NICHOLLS, B.Sc. (Hons.), LL.B. (Hons.), LL.M., MCIArb.

ALSO IN ATTENDANCE:
Mr. Pedro EASTMOND, (Clerk of Parliament)
Miss Suzanne HAMBLIN, (Journal Department of Parliament)
Ms. Rhea DRAKES, (Office of the Chief Parliamentary Counsel)

ABSENT:
Dr. Romel O. SPRINGER, J.P., MP., PH.D., (Deputy Chairman)
Senator Ryan O. WALTERS, M.B.A.

Call to Order
The Chairman called the meeting to order at 10:35 a.m.

Mr. CHAIRMAN: Welcome to Members present. Minutes of the Fourth Meeting, do we have them?

Mr. CLERK: We only have the transcript.

Mr. CHAIRMAN: We only have the Minutes of the first two meetings so far. This is the fifth meeting so obviously, matters arising from the fourth will be deferred as well. We are at Item 4 on the Agenda: Consideration of Written Presentations. We need to determined how to best manage this aspect. There are about 50 written presentations from what I have counted. Many of them are one-liners and some of them are repetitive.

Mr. CLERK: Mr. Chairman, please take a motion to have the Minutes deferred.

The motion that the Minutes of the Fourth meeting be deferred was put by Senator GREGORY P.B. NICHOLLS and seconded by Mr. PETER R. PHILLIPS.

Mr. CHAIRMAN: We need to discuss how best to manage these 50-odd submissions. Some of them were very short, and some obviously said the same thing. However, I have identified what I consider to be the key submissions. How do we propose to deal with those key submissions today?

Mr. CLERK: I suggest that the Committee, through you, Mr. Chairman, if you have taken out those particular ones, we can proceed submission-by-submission, and the Members can indicate how they view the submissions. If whatever has been proposed does not make any sense, we can decide whether it is something the Committee should consider or adopt, and so on. Mr. Chairman, I know you said at an earlier meeting that you are not taking any more oral presentations, but I have been reading the Bar Association's submission, and I am of the view that we should probably have the Bar come before the Committee. I am not sure what other Members think.

Mr. CHAIRMAN: Members would decide. I think what the Bar said is pretty clear; they do not need to expand. Clerk of Parliament, the whole thing is that the Senate has only given us another three weeks to submit a Report. I also understand you all are under pressure….

Mr. CLERK: That is true, but if the Senate has given that time and the Committee itself feels that, given the matters which have come before it, it needs more time to consider….

Senator G. P. B. NICHOLLS: Mr. Chairman, if I may help here, I have read the submission from the Bar Association and I believe that there are some useful suggestions we can consider. However, I also see in the suggestions or recommendations of the Bar Association a view that the Bill might be unconstitutional. I bitterly disagree with that summation. It is a misreading of the law. I know the author well. In fact, the author is the Chairman of that Subcommittee of the Bar Association and also a recently appointed judge, but I still think it is a misreading of the case of **Hinds v The Queen**.

Where I differ from that presentation, and I want to put it on the record, is that it submits that these offences under the **Cybercrime Bill** should not be tried by a magistrate, and that if they are not tried by a judge and a jury. In support of that submission, the committee of the Bar relies on the case of **Hinds v The Queen [1977]** which everybody learns in first year law when you start your programme at Cave Hill since the 1970s. It is totally at variance with what is said in **Hinds v The Queen** and I am not surprised that this mistaken view has been held.

Now, the Constitution provides that Parliament passes law for the peace, order and good government of the land, and nowhere in the Constitution does it delineate the jurisdiction between the High Court and the Magistrates Court. The Constitution does not say certain offences should be tried by a judge and jury and others by a magistrate. In the same **Hinds v The Queen,** Lord Diplock in giving the judgement of the Privy Council, explains that when they were looking at the constitutionality of the Gun Court, which was a court that the Jamaican parliament in the 1970s established to expedite gun crimes and matters dealing with firearm offences in Jamaica. The parliament wanted to establish this special court of three magistrates to sit and hear these gun crimes and offences, and the challenge was whether the Gun Court was constitutional.

The Parliament of Jamaica was purporting to take away the jurisdiction of the High court and vest it in magistrates. This is not the case here. This is a new Bill, a new legislative enactment which is creating offences that were not hitherto known to the law, so this is not taking away the jurisdiction of the High Court and vesting it in magistrates. That point was expressly set out in a much later case called **Suratt and Others v Attorney General of Trinidad and Tobago [2007]**, where the Equal Opportunities Commission of Trinidad and Tobago was established by an Act of Parliament, and the question was whether or not the jurisdiction of that Commission interfered with the jurisdiction of the High Court. In giving the leading judgement, Baroness Hale made the point that Lord Diplock never said that parliament was constrained in its ability to establish courts or tribunals or anything to deal with matters. The power of Parliament is not restrained by the Constitution. What Lord Diplock was saying was that you cannot take away the existing jurisdiction of the High Court and give it to any other body unless that body has the same measures of protection in terms of security of tenure and those matters that are dealt with in the Constitution.

Serious crimes are dealt with ordinarily by the High Court. There are some offences that are triable either way, where the accused person or the prosecutor would say, "We prefer to have this matter tried by the Magistrate," and the court makes a jurisdiction, and then the law also says some matters are tried summarily by magistrates. However, the Constitution itself does not get into that division. Who makes that determination? Parliament does, but what Parliament cannot do is take away the jurisdiction of the High Court and give it to magistrates who do not enjoy the constitutional protection of security of tenure. In this instance, in relation to the offences under the Bill which is under consideration by the Senate there is no interference with the judges' jurisdiction. Under the Computer Misuse Act, the jurisdiction was previously exercised by the Magistrates Court, if I am not mistaken, so when that Act was passed in 2004-2005, the jurisdiction was given to the magistrates to deal with. This follows that.

Mr. Chairman, I can well understand the policy of Government in not trying to clog up the court system at the High court level with these types of matters. I understand people may have some reservation where a magistrate might be able to fine somebody $70 000 on a summary conviction, but that in itself cannot make it unconstitutional because it was a jurisdiction exclusively exercised by the High Court before. Therefore, the Bar Association's position is plainly a misreading of **Hinds v The Queen,** and if you want to have an oral presentation, I would tell that to whoever comes from the Bar. Certainly, speaking from my reading of the law, I think that it is not unconstitutional for a Parliament to set up a method of determination of guilt in a Bill in the Magistrates Court. The Constitution is silent as to where the jurisdiction of the court is. I can perhaps some time later send the judgement and highlight the paragraph where Lord Diplock made the statement that is not in the Bar Association's report to us.

Mr. Chairman, I also hold the view that we can perhaps make an amendment to have it triable either way, which is a win-win. However, there is a reason why Government decides that, in creating a new set of offences under legislation, the court that determines these matters should be a High Court or a Magistrate's Court. There is a reason for that. These are summary offences.

Mr. Chairman, if the view is that the weight of the punishments is of such a nature that it should go, that is a question of judgement, but there is no legal principle here that is being trampled on. It is a question of judgement. Do you want these to clog up the court system with judge and jury trials? Quite frankly, we have that if a man slaps a woman on her bottom, that has to go before a judge and jury and not before a magistrate. Why? This is because it has always been so and we have never changed it. That is why the court system is clogged up every day.

Therefore, the policy of Government is that these matters should not be tried by way of a judge and jury. Now, if there is, and there can be, a case where, for example, malicious communication and cyberbullying are involved, if people feel that the one determination by a magistrate might not give sufficient comfort, even though there is an appellate process, they can appeal a magistrate's decision to the Court of Appeal and then to the Caribbean Court of Justice, which will ultimately have the final say. Fine! However, if you feel that it is too much for a magistrate, that does not mean that it is unconstitutional. It will be that there should be a preference that the gravity of the punishment should not be exacted without the benefit of a jury trial.

Now, we are also moving towards judge-alone trials. Therefore, what would be the policy that we are trying to follow? This is not a question of unconstitutionality. I find that the Bar Association's other comments are in line with many of the other submissions that we have received and even the concession made by the Minister on the last occasion. Therefore, these are useful. However, in response to the suggestion from the Clerk of Parliament, I do not think that we need to hear them or the Banker's Association, because their submissions are written with the highest degree of clarity and we can move on with our business. However, I defer to other members of the Committee if they want to.

Mr. CHAIRMAN: No, I agree that their submissions, whatever the merits of them, are clear. We do not need to have them orally.

Senator Nicholls, what would be your opinion on another aspect of the Bar's argument? Under Section 19 and 20, these alleged offences should be tried under the Supreme Court by a judge. You referred to it slightly, where they are saying that the penalty is steep. It is a fine of $70,000 or seven years imprisonment, or both maximum. What about bringing it down to $50,000 or five years imprisonment, or both. Does that make a difference in your opinion?

Senator G. P. B. NICHOLLS: The Bar had suggested $50,000 as an alternative, but that is just an arbitrary reduction. It is not based on any jurisprudential or legal philosophical basis. It is just that they feel that it is a little too high. However, who feels it knows it, and there are people right now in Barbados who are suffering as a result of these offences or these things harming them and their reputation on a daily basis. Therefore, it is the judgement of the Government that this is the appropriate fine. If we are going to take their approach, why not reduce it to half to $35,000. What is the difference between $35,000 and $50,000? Why not $20,000. We are going to get into this arbitrary arithmetical exercise where

we are just reducing for reducing sake, because we feel it too high.

However, the judgement of the Government, is that this Cybercrime is a serious threat to people's livelihoods, wellbeing, and welfare in the society. The punishments appropriately fit a maximum limit, because the court is not obliged to enforce the maximum punishment. This is not a mandatory sentence. The courts always have a plentitude of discretion in which to determine the appropriate sentence based on the facts and the circumstances before the particular court. To lower the limit, in my estimation, really can be unjust when you have a situation where the scope of the cybercrime between somebody who is just trying to actively destroy the reputation or hurt somebody, to where somebody is gaining some significant financial advantage from the cybercrime. You are limiting the scope of the punishment, and therefore you are going to narrow the culpability of the offender within a much narrower class.

Hence, the higher the fine, the more discretion the court appropriate punishment in the circumstances. However, when you narrow it, then you are lumping serious criminals with persons who are just interfering with persons, where culpability for those offences are not the same. Hence, in my view, I think that the $70,000 is not outrageous, because every court will have to make a determination, whether to give the maximum penalty or any penalty within that range. Lowering it then narrows the scope of culpability, where you might have a person who commits a truly outrageous act receiving the same or similar fine to somebody who does something that is not as damaging.

In my view, I will not agree with just a simplistic reduction of the maximum penalties under the Act. Thank you.

Mr. CHAIRMAN: What about what I had mentioned just now, making it an alternative as it is, for example, in Guyana? The malicious communication section could either be tried summarily or indictment.

Senator G. P. B. NICHOLLS: That would be a useful compromise. As I said, it would not be because I agree with the Bar Association's assessment that it is unconstitutional to have a serious matter or in any crime in the magistrate's court. If that were so, the magistrate court would not be able to handle any criminal work; everybody would bring a constitutional case and say the magistrate should not be doing this case.

Mr. CHAIRMAN: Are there any other opinions, Honourable Members?

Senator the Hon. L. E. NURSE: I have a difficulty because I do not know how, for example, the level of fines in this maximum number is determined. Is it a case where we say look at other jurisdictions and see what it is? Is it that we compare it with other crimes? I do not know. Possession of a firearm usually carries a charge of maybe $25,000 or whatever, and we try to look at these crimes and sort of hierarchy or whatever. I do not know how we come up with these figures because, quite frankly, at the end of the day, I really am not in a position to say if $70,000 is excessive or not? I do not know if anyone could expand a little bit on that.

Senator G. P. B. NICHOLLS: If I may help, Senator Nurse, Mr. Chairman, that is a very good point. That brings back to my mind what I said in the very first session. This legislation must be accompanied not only by the regulations which would govern its enforcement, but prosecutorial authority of the state must issue prosecutorial guidelines. I am aware that in Jamaica, for example, these same offences, the Director of Public Prosecution issues prosecutorial guidelines. Therefore, the public knows that if you do a particular act and you know that this act comes within the scope and meaning of the section, this is what the prosecution authority of the State of Jamaica will do in relation to this crime.

Likewise, the courts have to issue sentencing guidelines and should be encouraged. Parliament cannot make the court issue sentencing guidelines. However, I think the time has come for the courts to step up to the plate because there are three arms of Government: the Parliament, executive and the courts. The judiciary has to play its role. If a Cybercrime Bill is passed, the Parliament and executive should say to the judiciary that this is what is intended and therefore the Chief Justice and judiciary would determine the appropriate sentencing guidelines for judges or magistrates within a certain scope.

Certainly, it is not for Parliament to try to circumscribe how the courts would exercise that discretion. This is something that the courts would have to articulate on the basis, as you say, their knowledge and experience in terms of dealing with criminal matters, the impact on victims, the importance of the criminal statutes of the land to send a message as to what is acceptable and what is not, and those things. However, the guidelines for sentencing certainly are within the domain of the judiciary and the judiciary should be encouraged to set those guidelines.

As well, the prosecution should also issue prosecutorial guidelines so that a person doing something on the internet innocently without any intent or harm should know that even though the language is written in a way to capture offences or the manner in which offences are enacted, in a way that we want to make sure we capture all illegal activity. From that illegal activity that has not yet even been conceptualised, the prosecutorial guidelines would allow the public to know what is likely to make somebody find themselves before the court answerable to this offence, as opposed to something that is not.

For example, some of the concerns of the bankers' associations and the BARJAM could be assuaged by the prosecutorial guidance that is given by the DPP that these types of actions, for example, a caricature of a public figure in a cartoon that is posted online would not necessarily attract the attention of the prosecutorial authority, unless it is done with some intent to cause the person to alter their course of behaviour or from exercising a lawful duty that they might otherwise want to exercise or something like that. If it is done with some kind of menace or intent also. That is again now, the scope of the prosecution to articulate that.

Our job as legislators is to put the legislation in place to protect the interest of the public. However, the other organs of the State such as the prosecution which is totally independent from the State and is protected in the Constitution have to do its role. The judiciary which has to interpret the laws has to do their role as well to ensure that everybody, not only the alleged perpetrators of the crime but the victims of the crime, get justice.

I think we are losing a lot of that. We are trying our best to pass a law to protect the criminals but at the same time not giving due consideration to the victims of cybercrime. Therefore, we have to find, as I said, the correct balance. In doing so, the other arms of the State have to step up to the plate as well to ensure that this Bill when it becomes law is a law that is fair and balanced. That a person charged, innocent until they are proven guilty, will go through a system where they know fairly that this is the scope of the prosecutorial authority and if they are found guilty, then this is the scope of the courts' sentencing discretion.

I hope I have been able to satisfy you, Senator Nurse, but if I might just come back to your question, we cannot set the scope of sentencing. That is solely the discretion of the courts. They have to interpret the law and if there is a finding of guilt, they will fix a sentence. The accused man or woman would have the ability to appeal that sentence to a higher court. The appellate courts will then determine whether the sentence in the circumstances was disproportionate; it was excessive. That is how the system works. We cannot fix a perfect sentence because every crime or criminal act will have its own different set of circumstances.

It might be similar to another one in another jurisdiction but the court has to exercise its discretion on the facts before it. In relation to sentencing, I just want to reiterate that the penalty, as it is, gives a much wider scope for the courts to operate within. Once the courts give sentencing guidelines, judicial officers at the sentencing phase of the criminal matter will take those guidelines into consideration to affix the penalty in the appropriate place.

This is all that Parliament can hope for, but we cannot, at this stage, try to determine for the court what is the appropriate sentence for something as broad as cyberbullying, which can and will take place in varied and myriad forms. Therefore, that is not our role. We set what is the crime, what is the penalty and the courts have a margin in which they will operate to exercise that discretion.

Mr. CHAIRMAN: I think we dealt with the Bar Association submissions sufficiently. Let us continue with the institutional submissions of

BARJAM. BARJAM seems to be saying in some cases that the penalty is too high, but as Senator Nicholls said, I think that is within the ambit of Parliament to set the penalties they speak to, as one of their Members, Mr. Greene, when he came orally before the Committee on the Freedom of Information Act. We told Mr. Greene that is not our mandate, even though I certainly agree with him that we should have a Freedom of Information legislation.

Is there anything else that anyone gleans from the BARJAM submission? The Minister made concession on some words in Clauses 19 and 20. We would obviously examine that further. Therefore, I would propose that we do not need to examine them now. Is there anything else from BARJAM's submission that anyone would wish to raise for discussion? Of course, they spoke about the concern of freedom of expression. As I said, we would certainly discuss that further in our deliberations. If nothing else from BARJAM, let us go to the police service. Of course, before we move on to BARJAM, they raised concern from what I could see, about exemption from the media.

At least, they drew attention to the fact that the media is not exempted from liability. Good Morning, Honourable Leader of the Opposition.

Mr. CHAIRMAN: The media is not exempted from liability, and again, we can discuss that a bit further as we deliberate. I ask again, having said that, is there anything that anyone specifically wants to raise on BARJAM's submission? Okay, if not, the Police Service.

Mr. CHAIRMAN: Honourable Leader of the Opposition, what we are doing is going through the written submissions. We said we would work until about 1:15 p.m. or so and then we would have to agree on when next we will come back and further deliberate. We started with the Bar Association, then we did BARJAM, and now we are onto the Barbados Police Service. Is there anything from what they submitted?

Mr. R. A. THORNE: I am not sure if the question is directed towards me….

Mr. CHAIRMAN: No, Members generally. I do not think that they, at least from what I see, raised any issues for deliberation. They provided commentary, from what I am seeing, on Sections 19 and 20 of the Bill. Therefore, unless there is anything any Member wishes to further add on the Police Services Commission submission, let us go to the Barbados Bankers Association Incorporated

A comment I took out of their submission was that they recognised that offences were created where actions were taken without authority, and they were recommending that they be a definition of "without authority." Clerk of Parliament, I think that was one of the issues I asked you to raise with the Parliamentary Council. Regrettably, we have been told that no officer from the Chief Parliamentary Counsel's Office can be present today.

Mr. CLERK: She is on leave and will be back to work on Monday.

Mr. CHAIRMAN: Therefore, we would have to defer the decision on whether they would recommend a definition of "*without authority*" be included. Do any Members have any opinion on those words? The Bankers Association also referred to the fact that some Clauses, for example, *"transmitting data which causes substantial emotional distress" and "production of data for criminal proceedings"* they found to be broad and might hinder their prevention of disclosure of any information.

A note I had was that it is dealt with in terms of the Data Protection Legislation, which passed Parliament in the last term of Parliament. Hence, I did not see those as any major concerns that needed specific addressing in this Legislation. Were there any other institutional submissions? Did you see anything in there other than what I just mentioned? Okay, I do not think they were any other institutional ones. Right, okay.

That submission essentially stated there was not enough consumer protection in their opinion in this Legislation. My response is that this Bill is a general Bill on Cybercrime, and I do not know that it would be within the context of this Legislation to protect consumers. Their lobbying should, therefore, be directed towards the amendment of the Consumer Protection Legislation. Those pieces of Legislation, if I recall, were passed about 25 odd years ago, in the early part of this century or last century, and perhaps an argument could be made that they need

to be updated in light of all the technology that has transpired in those 20-plus years.

However, I did not think that the Consumer Association's submission that this Bill or Legislation should deal specifically with Consumer Protection had merit concerning this Bill. However, other Members, if you have a contrary opinion, please share. Okay, if not, let us go to some of the individual submissions. Mr. Neil Harper, of course, gave a written submission and then followed it up with an oral presentation, but we do not have the oral presentations available as yet. Is that is correct, Clerk of Parliament? Do we have oral submissions from, Mr. Niel Harper?

Mr. CLERK: What he submitted is the presentation that he made, but obviously, we do not have our interaction with him.

Mr. CHAIRMAN: Right, but he then submitted a written presentation as well.

Mr. CLERK: What he presented orally, he also sent in writing.

Mr. CHAIRMAN: He sent it in writing then, yeah. Okay, so he was the first to give a written submission. Can we agree to take his now, or do you want to take his later since his is one of the most substantial and, of course, pretty technical. Do we need to have the Parliamentary Counsel present to go through his properly, in which case we defer, or do you want to take his now?

Senator G. P. B. NICHOLLS: I would have preferred to have a little more time to digest his presentation and to have the Parliamentary Counsel present.

Mr. CHAIRMAN: Yeah, I think we agree.

Senator G. P. B. NICHOLLS: There are some presentations, for example, where, if we get to the stage where we want to make amendments to the Bill, we should do that when Parliamentary Counsel is present. His presentation is one that makes such suggestions. I am not necessarily in agreement with everything he says. For example, when he mentions a specialised court in England called the King's Bench Division, we had a King's Bench division in Barbados, but in 1981, we removed all of those divisions with the Supreme Court Act and modernised the law. The King's Bench Division is not a trained division in technology law, but England is a big country, and they may be able to roster judges with certain areas of expertise.

There are times where I think he has made valid comments that we should consider, but others are slightly outside of the scope of what we can do in this jurisdiction. Therefore, I would like to consider his submissions when we are dealing with any amendments and when we have Parliamentary Counsel present.

Mr. CHAIRMAN: I agree. Let us move on to Stephen Williams. Remember, he was a consultant to the Law Reform Commission, so from what I analysed, his submissions were generally in favour of the Bill as presently drafted. In his written submission, he proposed that the definition of cyber terrorism be expanded, but then when he came before us orally, he withdrew that submission. He recommends that the critical infrastructure service provisions in Clause 12 be placed in Regulations for easier amendment. Of course, having them in Regulations would not necessarily make them more easily amendable because in Clause 12 it speaks to the Minister having the authority to make amendments by negative resolution, essentially in the Official Gazette, adding to it.

What I certainly believe and would propose is that we expand this list of critical infrastructural services, because it looks too narrow to me. If I may place on record from here for Members' consideration, I am of the opinion that added to this present list, services such as confidential educational material, for example, examination materials like CXC materials and the Common Entrance Examination materials, should be added because they are critical. Public transportation, utilities such as water and electricity, essential public infrastructure such as hospitals, law courts, traffic lights, the air and sea ports, as well as banking and financial services, are so vital that any incapacity or destruction of their computer systems or data would have a debilitating impact on our national security: Economic security, public health and safety and international relations of the State. That is what I would propose, and I am putting it out there for Members' consideration at a later meeting, but I did not see anything else from Stephen Williams' submissions to engage the Committee. Unless any Members differ, we can move on to some of the more general ones.

A lot of them together spoke towards Sections 19 and 20 of the Bill being too vague. Like I said, we can deal with that. We had the Minister who came before us to propose taking out some words, so we certainly would need to deliberate on that; the issue for Sections 19 and 20 being provisions which seek to curb the constitutional right to freedom of expression. Many of them spoke to that issue. Senator Nicholls, I believe you have a proposal on Section 20. The claim by Dave Weekes orally and some of the critics of this Bill as presently drafted is that it is being done to protect politicians and their friends. I think those were Mr. Dave Weekes' exact words. Is there any Member who would wish to comment on that and to put on the table a possible amendment to Clauses 19 or 20 or both?

Senator Senator G. P. B. NICHOLLS: Are we dealing with specific amendments now, Mr. Chairman?

Mr. CHAIRMAN: We are dealing with the written submissions, and quite a few of them expressed that concern and criticism. Otherwise, do we just continue going through them and try to take out what they have said.

Senator G. P. B. NICHOLLS: Mr. Chairman, as I have said, I have looked at all of the submissions, and I have read the majority of them, especially the ones that come from the institutions and Mr. Harper, and so forth. I think that we can have the Report written in a way to expedite this process. We do not necessarily have to go through each and every one of the submissions, but we have received submissions from the public which spoke to issues relating to freedom of expression, the vagueness of the language, the broad nature in which the language is written, the uncertainty as to whether or not these terms can be subjectively identified by the members of the public as something that is a criminal act, and so forth. We can go through these in a summary way rather than us now trying to sift out what each individual would have submitted.

Mr. CHAIRMAN: Right, that was why I brought to the meeting one of the main criticisms, namely concern about a curb on the freedom of expression. If we wanted, at this stage, to propose any response to that….

Senator Senator G. P. B. NICHOLLS: Sir, I would basically submit that the right to freedom of expression is not a right that is given in absolute terms. The Constitution, at Section 20, provides for laws to be passed to limit that expression, provided that those limits are reasonably required in the public interest and also to secure the rights and freedoms of others. The intent of the Bill is not to unduly restrict people from expressing themselves, but from doing so in a manner by way of electronic means on the internet that would interfere with other persons, or is likely to cause harm or effect change in the conduct of persons by way of some malicious or oppressive actions. To that extent, the law does not interfere with anyone's constitutional rights.

The question in determining whether the limits that are being imposed. The first question is that the law can stand to impose limits on speech, so that is the first hurdle. Therefore, the next question is whether or not the limits are proportionate to the objective of people enjoying the fundamental right of freedom of expression. That is where the discussion has to go in terms of how far can the Bill go. Does the Bill go too far in curtailing that freedom of expression? Therefore, when we line up the provisions of cyberbullying and malicious communication, these are the two that have attracted a lot of the public debate and concern. Our question is, do we have a provision in regard to both of those elements, cyberbullying and malicious communication, et cetera? Have they gone too far? Is it a less intrusive means by which we could achieve the very important objective of securing people from harm and danger by way of cybercrime? That is the test. That is where I operate in terms of looking at the Bill. That is just to answer the concerns by members of the public that the Bill simpliciter is an incursion on their freedom. The answer to that would be yes, but the Constitution does permit incursions on your freedom, provided that there are in the public interest and the rights and freedoms of others are respected. Therefore, that balance has to be drawn.

Mr. R. A. THORNE: I think the time has come when this must be placed on the record. I have heard in here and I have heard in the Parliament, in the House of Assembly, this statement that we have freedom of expression in Barbados and we do not have freedom of speech.

I think that as lawyers, and for non-lawyers, we need to erase that statement from the public record. When it is made by parliamentarians, especially by parliamentarians who are lawyers, and when it is made by parliamentarians of considerable experience, and when it is made by parliamentarians who chair Committees, I am begging you, Mr. Chairman, to have that proposition in law permanently removed from the record.

I repeat, the statement has been made here, and it has been made in House of Assembly, to wit that the Barbados Constitution makes provision for freedom of expression and unlike the United States, it does not make provision for freedom of speech.

I am trying to find the most polite way to correct that, to say that that is a statement that is entirely and egregiously erroneous in law. Freedom of expression is the generic term that includes freedom of speech. Therefore, let me seize this opportunity to ask you, Mr. Chairman, to erase that proposition. If it remains a proposition, it is false, it is wrong, and it is entirely correct for this Committee to convey that statement to Barbadians. I would ask that the earliest opportunity be chosen to correct that.

We do have freedom of speech in Barbados. We have freedom of expression in Barbados. Perhaps it is a question of language, it is a question of nomenclature. However, please no longer let that statement go abroad from this Parliament.

Mr. CHAIRMAN: Let me ask, because I know Senator Nicholls also expressed similar sentiments. I certainly do not propose that I am any expert whatsoever on United States law in terms of their constitutional right to freedom of speech.

However, let us expand on this and let me give examples, at least as I understand it. Once there is a public figure, a politician, or President, you could say virtually anything about them. You can say they are crooks, they are corrupt, et cetera. You do not even have to prove that it is true, and of course, you are saying in public, outside of the House of the Congress, et cetera. Whereas in Barbados, for example, if you were outside the confines of Parliament and say that XY Minister of Government is a crook, a fraud, or is corrupt, and you cannot then prove it in court or it does not come within the purviews of comment either, you can be liable.

Let us expand and enlighten me as to what I perceive to be the difference between the freedom of speech as constitutionally accepted in the United States and freedom of speech as under our Barbados Constitution.

Mr. R. A. THORNE: Senator Nicholls spent some time pointing out what is correct in law, that when a freedom is granted, even a fundamental constitutional freedom is granted, the Constitution always derogates from that right, which is in keeping with the political philosophy of John Stewart Mill, that freedom is not the right to do what you want to do, but the right to do what you ought to do.

What you have just discussed is not a difference between speech and expression. What you have just discussed is a difference in interpretation. Within the political and legal culture of the United States, the courts there have extended the freedom of speech beyond the boundaries that are extended here in Barbados. In other words, the United States offers a more liberal dispensation than Barbados. You have the Enquirer Magazine; you have the right to freedom of expression or freedom of speech, which I am using synonymously. It is liberal in the United States; it is not liberal around here.

I will give another example, a cultural example. You probably have attended calypso tents in Trinidad. If you attend a calypso tent in Trinidad, what you here there, the liberal expression in terms of criticising politicians and public officials, you do not hear it here because it is a different cultural tradition. Barbadians are more careful with their speech. They are more cautious generally, in terms of making assaults on people's character, their reputation and record of service. You do not find that in Trinidad. In fact, the calypso tent in Trinidad serves as an exclusive zone where it is felt that calypsonians and masters of ceremonies can say what they want to. There is a tradition that they do it with some immunity. Now, it does not stop a person from suing a calypsonian or a master of ceremonies in a tent in Trinidad, but they do not do it. They do not do it because a person who sues a master of ceremonies or a calypsonian is risking his career because it is

felt this is the season of truth. This is the season of the poet also known as calypsonian. People feel that they are telling the truth. They feel that if you bring litigation against them that you are trying to hide the truth. This is why people do not sue in Trinidad. The same does not apply here. We have a shorter tradition. We have only been doing this for the last 45 years. The Trinidadians have been doing this for a long, long time. Therefore, it is a tradition. It is a pattern of cultural behaviour that finds more liberal expression in Trinidad. It is a pattern of more liberal political and legal interpretation that influences the law in the Unites States (US).

Really it comes down to interpretation. It comes down to constitutional interpretation, as to what is freedom of speech/ expression. It comes down here to what is permissible. Hence, that is the distinction. It is one of interpretation in terms of the cultural thing between Trinidad and Barbados. It comes down to what is permitted. They permit it in Trinidad. They do not permit it here. There, it is two systems operating differently. Two systems behaving differently in terms of their treatment of speech and expression. That is, it.

Senator G. P. B. NICHOLLS: Mr. Chairman.

Mr. CHAIRMAN: Senator Nicholls.

Senator G. P. B. NICHOLLS: When I heard the comment made here, because I would not necessarily have the time to listen to the debates in the Other Place, I understood you to mean that the freedom of expression that we enjoy in Barbados is not the same as what people would understand and appreciate as the freedom of speech that is enjoyed by Americans under their Constitution. I think it would be the Fourth or Fifth Amendment of the Constitution. I am not sure which amendment of the American Constitution but actually, in strict terms, it is not the freedom that is actually set out in the Constitution.

It is set out in one of the amendments. What is more important, and I am glad that the Honourable Leader of the Opposition did draw the reference of Trinidad and Tobago, is that, like the American constitutional freedom of speech, the Trinidadian provision does not have any written limitations in the constitutional text. The rights are expressed simpliciter. These are the rights. No limitations. Derogations or limitations on their rights. Therefore, there is no expressed or textual derogation or limitation on the right.

In the case of *Panday v Gordon* (2005) UKPC when Mr. Panday had criticised the publisher of the Guardian newspaper in a most deplorable way, the argument was made that the Constitution of Trinidad and Tobago did not set out any express limits on the freedom of expression, and therefore Mr. Panday was entitled to say what he wanted to say against Mr. Gordon. The Privy Council in its judgment, which is still much quoted today, indicated that the freedom was not absolute. Even though Parliament did not prescribe a limitation in the text of the Constitution to the extent to which that freedom could be enjoyed, it was for the courts to determine the limits.

Therefore, even in recent times, that argument resurfaced when the COVID-19 cases went to the courts and in the Privy Council in a case called *Dominic Suraj and 4 Others v Attorney General of Trinidad and Tobago* (2022) UKPC where there was some misunderstanding as to whether or not there could be any limitations given by the courts on fundamental rights and freedoms. The Privy Council again, as recently as two years ago, restated that these rights are not absolute. To the extent which rights are absolute in the US, that is not necessarily true either.

There is a lot of litigation to protect the freedoms of persons' reputations that are harmed by speech that is made in the political sphere and otherwise. We do not see a lot of the reporting of it because obviously we are limited to the political theatre that is provided by the networks we are forced to watch. However, I understood your comment, Mr. Chairman, that the freedom of speech that does not exist, you meant there was no unbridled freedom of speech as might be the case in the US where the Constitution does not prescribe the limits and extent of that speech.

That is how I understood it. I move very quickly to scotch any notion that you might be saying that there is not freedom of speech in Barbados. I understood you to mean that there was not freedom of speech within the same context as is provided within the American Constitution.

Mr. CHAIRMAN: That is exactly correct.

Senator G. P. B. NICHOLLS: That is why I meant to correct it at the time. The Honourable Leader of the Opposition is right to bring it up here again, so that we can have some clarity. However, I understood your position to mean that it is not a freedom that is enjoyed in the same way that is enjoyed in America, and not that Barbadians do not have freedom of speech. I know that operatively your comment might be the subject of some gist for a different type of **inaudible**. Last week, next week, or in the future, but certainly I think that your position can be properly defended, if necessary.

Mr. CHAIRMAN: That is why I raised the issue.

Mr. R. A. THORNE: I hope Senator Nicholls will send you a bill, and I would urge you to pay it hastily.

Mr. CHAIRMAN: That is why I raised the issue. What I see going on in the US, for example, when the then candidate Trump was running. What election would that be? The 2016-election against the then candidate Hilary Clinton. You know, how he used to call her all of the time; crooked Hilary and that kind of stuff that certainly would not be allowed here. However, that leads us to the issue as to whether the Committee feels or would wish to propose some kind of subject to issue for Clause 20. Clause 19(3) has the defamation defences; truth, comment, qualified privilege, absolute privilege and triviality. However, Section 20 does not have any defences at present. Would the Committee be minded to consider proposing that there be some protection for persons who may otherwise be guilty of cyberbullying, if it does in terms of political satire? Honourable Leader of the Opposition, you referred to tents in Trinidad. Yes, we went to law school there and know about that, for instance. However, is there any way that Members would wish to consider such a proposal that there is no liability if it is within the public interest to put forward this image or the public's attire or newspaper image. I do not know. I am just throwing that out there.

Senator G. P. B. NICHOLLS: Mr. Chairman, I discussed with you yesterday, and I have looked at a number of different pieces of Legislation from around the world on Cyber Bullying. Interesting I am not really seeing any definition of Cyber Bullying across the various jurisdictions. In Canada, for example, the Criminal Court speaks to these things. I visited the Justice Laws Website of the Government of Canada and there is no definition of what it is, but it can tell you what is Cyber Bullying. In other words, it is not defined, but it can tell you what falls within the scope of the Legislation, I should say. But to my mind, what is important is that we need to give the drafters the latitude or respect that the drafters have framed the section with a sufficient degree of latitude to capture what, in essence, is a very pervasive criminal act that is occurring, but at the same time, trying to frame that within the context that we cannot at this time conceive of all of the possible methods by which this Act can be pursued. Cyber Bullying is bullying using the technology, and what is bullying? I am not necessarily sure that we have captured the essence of what bullying is within the Legislation, and we have used the models from other jurisdictions. Jamaica has it, Guyana has it and the draft laws. Bermuda just passed the Cyber Crimes Bill last week.

Mr. CHAIRMAN: They are calling it Computer Misuse. The old name that we have or the present name we have.

Senator G. P. B. NICHOLLS: So for me, let us go back to school and what we did at school to younger boys who we tolerated toady by any stretch of the imagination, but people were arguing that the schools were more orderly then and that the teachers did not really have to come out the staff room at lunch time or at break to supervise the schools in a way which they probably have to do now. But what is bullying? Bullying could be physical, it could be fear that some force might expel against you, and you know what is bullying? I would like if the drafter is present for them to reconsider trying to give a more concise definition of Cyber Bullying. If it needs to be written in a broad way, but it must start from a root position as to something that necessarily is trying to unduly cause someone to change their course of conduct or their pattern of behaviour or the decision that they would want to make by the use of some threat or intimidation. That should be in essence what Cyber Bullying portrays. When we use words like intimidate, embarrass, anxiety, those are the effects of Cyber Bullying, but in essence, I think that we should

try to use our best efforts to define it in a way that is broad enough to capture some act that is threatening someone to change their course of behaviour or making someone apprehensive about bullying or thinking something or saying something or participating in a group activity or something of that matter, and that we can at least try to find a more workable definition for Barbados of what Cyber Bullying is. But Mr. Chairman, I have not seen in the Criminal Court in Canada, for example, where it says Cyber Bullying hurts the other people can change lives. Some actions taken when Cyber Bullying occurs can also be against the law, but Cyber Bullying itself is not one of the Criminal charges for which someone can face in Canada, but it is mentioned here on the Canadian website so it is not as I said defined in a way. They are more specific; for example, they have sharing intimate images without consent, criminal harassment, uttering threats, intimidation, mischief in relation to data unauthorised of computer identity theft, extortion, false messages, indecent or harassing, harassment, counselling, suicide, incitement of hatred defamatory liable, public incitement of hatred, offense against the person and reputation. They have labelled all of this as elements of Cyber Bulling but they are individual offences so they have not tried to define it by using the broad language that we have used but we have a much wider scope and range of offences that fall under the general head of Cyber Bullying better than having it in a section with the broad language that we have they have actually broken it down into one, two, three, four, five, six, seven, eight, nine, ten, eleven, twelve, thirteen, fourteen different aspects that are more particularly defined.

Mr. CHAIRMAN: What Legislation is that?

Senator G. P. B. NICHOLLS: This is the Canadian Criminal Code. Okay, wait, let me come back out here. Hold on a minute. I am on the website of the Government of Canada, and I goggled Cyber Bullying and the possible criminal charges in relation to Cyber Bullying under Canada's Criminal Code, but Cyber Bullying itself is not defined as one of those charges. But under the broad head of Cyber Bulling, they are 14 different offences, so it is the Criminal Code 1985 in Canada.

Mr. CHAIRMAN: I would have imagined they have more up-to-date Legislation than that, so we will have a look and do the research.

Mr. R. A. THORNE: Just to clarify, is this going back to the House for debate?

Senator G. P. B. NICHOLLS: It goes back to the Senate as a report, and if the Senate adopts the report of the Committee which includes changes to the Legislation, it will ultimately have to come back to the House.

Mr. R. A. THORNE: To the House, right?

Mr. CLERK: Only the Amendments.

Senator G. P. B. NICHOLLS: The more I see this evolving, the more I am convinced that it needs to be pared down a lot more than we are thinking. I want to defend the right of the sycophants and the agents of the government who are out there right now insulting people because the irony is that the Government is in this place, and I do not mean in here. The Government is in this place trying to pass a law to stop people, to use Senator Nicholls' broad term, Cyber Bullying people. I would just say this in way of an anecdote and to make the point that I saw a video this morning which is an excerpt of these proceedings. The lady took that and she called me a rat. I found it very funny, by the way, deriving from my initials R-A-T, and she said "he is rude, aloof, and toxic". I think she has the right to do that. The irony is that she is a sycophant and an agent and a hireling, and I used the word "hireling" deliberately because these people are getting money and small jobs to insult and curse people. While her government is trying to pass a law to prevent people from being, she goes on social media. I find it funny because I am not sensitive. I am in politics and I expect it. I even invite it, because if she wants to give me mileage and publicity, fine, I will take it, but when I saw it this morning I said: Is this not ironic?

I am supposed to take offence and I am supposed to crawl under a hole, and I believe that this Government – I hope you do not mind me being political – as stated by the immature little fellow is trying to protect its Ministers and its parliamentarians and its public officials from doing precisely what that blogger is doing in relation to me; and I do not mind. I would go into the public domain and I would defend her right to insult me, to cyberbully me. Yet here we are going

over legislation that intends to stop her from doing what she is doing. Is that not very ironic? That is why I feel that in the evolution of things, this law is becoming a very dangerous law. I am not so sensitive that I would want her to stop. I found it funny. It is part of the political struggle that people insult each other, but we in here in this Parliament are trying to stop people from insulting each other.

Mr. CHAIRMAN: So, Honourable Leader of the Opposition, what is your proposal then on that Section?

Mr. R. A. THORNE: My proposal is that Section 20, which prescribes so many categories of speech – ordinary, muscular speech, as they call it – criminalises that kind of thing. I suppose a man can go at a meeting and curse somebody, but can he not go on a computer and curse somebody? I think that section – if you say Section 20, Mr. Chairman, that is it, I was appalled when I saw it, because no speech now is allowable, no speech now is permissible, no speech that attacks the other person is allowable. I am not advocating for personal attacks. I go on principle. I have never attacked anybody in this Parliament or outside personally. That is why I think that unless you elevate the standard of speech – and a lot of people do not because a lot of people make a political livelihood insulting others – can you pass a law to stop them? I do not think you should pass a law to stop them. I think the ultimate judge should be how the public views them as people who are incapable of raising the standard of their debate. However, for the others who cannot raise their standard of debate- including people who come in there every Tuesday – let them continue. Let them continue and let the public judge them, but criminalise them if they go on a computer? No, I do not think you should. So I think that section needs to be worked on.

Senator G.P.B. NICHOLLS: Mr. Chairman, before you go there, I just want to respond. I am not necessarily disagreeing with the Honourable Opposition Leader. I actually agree with what he said, and it raised some eyebrows in here when I said that I believe that under the Constitution of Barbados, under the democratic society that we live in, a person has a right to say something that is offensive, a person has the right to say something that is obnoxious, a person has the right to say something that offends people. Where we have drawn the line is where that offence or that obnoxious statement is not intending harm to someone else. That has always been the standard, and a line has to be drawn.

Asides.

Senator G. P. B. NICHOLLS: The society also has to protect people who can suffer harm as a result, and I think that is what we are losing by the over-indulgence in what happens to the political class as a result of the passage of this Bill. It is not only defamation, because at the end of the day I know of instances where at least three people committed suicide as a result of cyberbullying last year in this society. In our use of the political class as an example of how it would relate, I think that if we do not create an offence of cyberbullying, there would be too many people that are harmed in this society as a result of it.

Asides.

Senator G. P. B. NICHOLLS: I want to respond to Ralph's point, and that is why I feel that there might be some merit in broadening the scope of the cyberbullying by delineating the elements of cyberbully similar to how the Canadians have done it, without trying to use it as a broad omnibus provision. I am looking at it here, but I want to do some more research. This is within their Criminal Code generally. Under Canada's Criminal Code, I think what they have done is whether this is done online or in print media, these are criminal charges under their code. So, cyberbullying, according to the Canadian government, is unlawful if you engage in any of these acts if you do them online.

When you look up cyberbullying in Canada, it points you to possible criminal charges, sharing intimate photos; anyone knowingly publishes, distributes, transmits, sells, makes available or advertises and intimate image of a person, knowing that person depicted in the image did not give their consent to that conduct, or being reckless. It does not necessarily speak to what happens on the Internet. It is much broader. In other words, as you just pointed out, something that I can say to you is not a crime, but if I do it on the computer, it now becomes a crime.

Mr. R. A. THORNE: Very specific there, what you just read. So it is an intimate photograph, an intimate and consensual photograph.

Senator G. P. B. NICHOLLS: Yes, so that is probably publication of an intimate image without the consent of the other person.

Mr. R. A. THORNE: Yes, originally consensual but, classic situation, they break up and you publish it.

Senator G. P. B. NICHOLLS: But if a photograph is taken without your consent and you are not aware of that photograph, it would seem to me that this Section does not provide the cover for it. I can hide a camera and you can be in a place and not know that a photograph or video is being recorded.

Mr. R. A. THORNE: But what do you think of the Section, with all of those categories of speech?

Senator G. P.B. NICHOLLS: My thinking is that we need to have a better definition of what is cyberbullying if we are going to use it as a crime.

Mr. R. A. THORNE: Sorry, Senator Nicholls. Are you saying we should replace Section 20? You would keep Section 20?

Senator G. P. B. NICHOLLS: I would keep Section 20 but it would have to be changed. It has to be amended, in my view.

Asides.

Senator G. P. B. NICHOLLS: Make provision for cyberbullying. Section 20 deals with Cyberbullying.

Mr. CHAIRMAN: Let me ask this question. Section 20 also has about pornographic and indecent data, so do we agree that a person who intentionally uses a computer system to publish data that is pornographic should be liable if they are publishing it to humiliate or intimidate someone?

Senator G. P. B. NICHOLLS: Mr. Chairman, I do not think we have a difficulty with that.

Mr. CHAIRMAN: Right, because you all said "offensive" and that can come out, but in terms of the pornographic and vulgar and profanity….

Senator G. P. B. NICHOLLS: I think that should be an offence in and of itself. That is the point I am making, that we can look at the cyberbullying section we have there and take out those like how the Canadians have done.

Mr. R. A. THORNE: Paragraph (b) is the one we are talking about.

Mr. CHAIRMAN: They are together. There is no "or". It follows on from (a).

Mr. R. A. THORNE: As with the Sexual Offences Act, last year when Justice Weekes struck it down. She struck down gross indecency against a child because it was drafted like this, because it was put into one section.

Senator G. P. B. NICHOLLS: Indistinct.

Mr. R. A. THORNE: Therefore, this is a mistake in the drafting here. These need to be separate offences altogether. It just causes for one being….

Mr. CHAIRMAN: I am very sorry that there is no Parliamentary Counsel here today to try to say how it is sorted out.

Mr. R. A. THORNE: I am saying that (b) is the problematic one. How to do you charge somebody for causing an inconvenience or insulting, or humiliating or intimidating? That is many people's political performed speech.

Senator G. P. B. NICHOLLS: I think her approach to that is that….

Mr. R. A. THORNE: She instructed.

Senator G. P. B. NICHOLLS: No. This is a drafting error.

Mr. R. A. THORNE: A sensitive Government.

Senator G. P. B. NICHOLLS: I do not agree with that categorisation at all. The (a) and (b) are not conjunctive. I think (b) is a qualification and I think that is the intent.

Asides

Mr. CHAIRMAN: I am reading them as being together, because it does not say, "or". Therefore, let us say you are publishing pornography for the purpose of humiliating a person.

Senator G. P. B. NICHOLLS: I think that is badly drafted. Therefore, a person who intentionally uses a computer system for the

purpose of causing a noise, inconvenience, danger or obstruction is not an offence. The way this is intended is to follow a qualification. That is the intent.

Mr. R. A. THORNE: A semicolon appears at the end of (a); Why does a semicolon appear there? This is because (b) is a separate offence. Look at it.

Senator G. P. B. NICHOLLS: I understand that, but the draft lady is not here to defend.

Mr. R. A. THORNE: She will have to resolve it.

Senator G. P. B. NICHOLLS: I suggested that this section should read, "A person who intentionally uses a computer system"…

Mr. R. A. THORNE: (a) that is an offence, (b), that is another offence.

Senator G. P. B. NICHOLLS: If that is the intent I do not agree with it.

Mr. R. A. THORNE: Me neither.

Senator G. P. B. NICHOLLS: Therefore, that is why I am saying that we should….

Mr. R. A. THORNE: Senator Nicholls, every punctuation has meaning and I see a semicolon there at the end of sent.

Senator G. P. B. NICHOLLS: What he is saying there is no 1(a) or (b). There is no 'or'.

Mr. R. A. THORNE: Why the semicolon? Why not a coma?

Mr. CHAIRMAN: I believe they are the two together.

Senator G. P. B. NICHOLLS: Mr. Chairman, I will say this. If you have a law that says a person who intentionally uses a computer system for the purpose of causing annoyance, inconvenience, danger, obstruction, embarrassment, insult, injury, humiliation, intimidation, hatred, anxiety; some of these things are reprehensible, some of these things are borderline, some of these things are nebulous and trivial. I do not think that you can use a computer system for the purpose of causing hatred, because hatred can lead necessary to danger or some action that can put people's lives in danger. If I want to annoy somebody, should I be allowed to use a computer system to annoy somebody? I do not think so.

Mr. R. A. THORNE: All from the Computer Misuse Act. All repeating what was in the Computer Misuse Act.

Senator G. P. B. NICHOLLS: Exactly.

Mr. R. A. THORNE: These were offences before.

Senator G. P. B. NICHOLLS: Right, but the thing about it is that I think we got the opportunity now to get the drafting right. Therefore, whereas the Canadians have identified what are the particular things that are criminal offences.

Mr. R. A. THORNE: Ask Minister Caddle what she intended. If she intended two separate offences or for this to read as one offence? Looking at this it looks like two offences.

Senator G. P. B. NICHOLLS: Even if (b) is read as a qualification on (a), I do not think that that serves the purpose. I want to know that sharing and intimate image without someone's consent, recording somebody without their consent, uttering threats on the computer, intimidating people on the computer, stealing their identity, trying to extort them. Mr. Thorne, we have a colleague that for months an intimate video of him was recorded of him without his knowledge, and for months was being extorted out of money.

The harm and danger that this does to people, outside from trying to decide what is going on in the political class, extortion, false messages, indecent harassing telephone calls, emails, and messages and those kinds of things. These are crimes. Suicide, telling people they should go and kill themselves. That does not really happen a lot in Barbados, but in terms of beauty pageants, body shaming people. This is criminal activity, whether we like it or not, this is criminal activity and we need to draw the line.

However, the broad way in which cyberbullying is put there for the convenience, I believe of the drafters, to have this very broad section, just general language, does not cut it for me. If this is a crime, say it is a crime. Defamatory, liable, public incitement of hatred,

things against people's person and their reputation and that kind of stuff. If that is a crime that is a crime. However, lumping it together as this broad omnibus term called cyberbullying in itself is not necessarily definable in law. In other words, the common law does not know what cyberbullying is. We are creating a statutory offence of cyberbullying, but we are still using very broad language, which captures a lot of the cyberbullying crimes, but also might bring in the net, thing that are nebulous and trivial, such as I said, political caricature, which is what Mr. Thorne enjoyed when he saw it this morning, as oppose to something that is inciting hatred.

Now, do not be surprise, we can get there. I was listening to a BBC documentary on the people who were incited to kidnap the Governor of Michigan, Gretchen Whitmer. Now, these people were motivated by things on the internet that the algorithm was putting this thing directly in their social media feeds, because you click on certain things, the algorithms decides that you like these kinds of stuff and they were motivated to capture her and to take her to some place in another State and have trial which was only going to result in her death, and they were motivated by that. Now, somebody that is putting it into some unsuspected **inaudible** that kind of information in their social media feeds, where they believe that the people of political parties molest children and that kind of stuff. How do you protect the public from that kind of behaviour? Now, it might be used to whip up political support, but some people are on these threat, so how do we draw the line? We cannot just throw away cyberbullying because we do not want political criticism, but at the same time, I feel the way to save the people who are subject to these offences, is to delineate the specific aspects of cyberbullying in more detail, rather than having a broad omnibus turn to do so.

Mr. CHAIRMAN: Okay. Senator Nicholls, you said you will try to find a definition?

Senator G. P. B. NICHOLLS: I do not think it is a term that the law wants to define, because once you define it, when an Act that is so egregious falls outside of the margin, then there is no law against it. Therefore, that is why it is not defined. It is an intent not ….

Mr. CHAIRMAN: I think we still agree that the publication of pornographic material for the purpose …

Senator G. P. B. NICHOLLS: … Without a person's consent.

Mr. CHAIRMAN: Right. "Cause them humiliation" should be and that is one example of what should be in.

Senator G. P. B. NICHOLLS: Because, Mr. Chairman, if I published pornographic material and the person does not have a problem with it, how can it be cyberbullying?

Mr. CHAIRMAN: Without consent. For the purpose of causing humiliation.

Senator G. P. B. NICHOLLS: So, that is why (a), Mr. Thorne, has to be read with (b).

Mr. CHAIRMAN: Yes. Yes.

Senator G. P. B. NICHOLLS: Because if you….

Mr. CHAIRMAN: I think that that is the intention.

Senator G. P. B. NICHOLLS: If people are at university or something is engaging in some kind of sexual act and records it, and you read (a) separate from (b), a person who publishes a pornographic material can be guilty of an offence simpliciter. It would have to be that (a) has to be read with (b) for the purpose. So, the purpose. The way in which it drafted is not clear. I understand why you are saying that the…

Mr. R. A. THORNE: **INAUDIBLE** Any person who intentionally uses a computer system for the purpose of….

Senator G. P. B. NICHOLLS: But, if you read Clause 20(1)(a), "and is guilty of an offence", it would not make sense either. If I put a boy and a girl at a fete "wukking" up, her breasts exposed and that kind of stuff. Some people might consider that as vulgar but if you publish that simpliciter, you cannot be guilty of an offence. You "wukking" up at a fete and panty exposed, some people might consider that vulgar. But, it would be if you were doing that for the purpose of causing an annoyance, an inconvenience or a danger, that is when the act becomes criminal. So,

that is why I am saying I do not necessarily read (b) as a separate category of offence.

Mr. CHAIRMAN: I think the intention of the draftsman was that they be together. So, like I said,….

Senator G. P. B. NICHOLLS: Mr. Thorne, you are inclined to have that….

INAUDIBLE

Senator G. P. B. NICHOLLS: If I put online somebody "cussing"….

Mr. R. A. THORNE: Somebody cursing?

Senator G. P. B. NICHOLLS: Cursing. That is an offence? That is cyberbullying? If I publish John Brown down town cursing, a person who publishes somebody who is cursing or saying something menacing, without the purpose of annoying somebody, intimidating, inconveniencing or causing danger or obstruction; without (b) that itself cannot be a crime.

Mr. R. A. THORNE: No. But, data. It talks about data and whether it is offensive, pornographic, indecent, vulgar….

Senator G. P. B. NICHOLLS: No. No. I am ….

Mr. R. A. THORNE: You are saying photograph. If I take a picture of you….

Senator G. P. B. NICHOLLS: "Cussing" somebody about cricket.

Mr. R. A. THORNE: And I put….

Senator G. P. B. NICHOLLS: Let we say cussing about cricket.

Mr. R. A. THORNE: I beg your pardon.

Senator G. P. B. NICHOLLS: Let us say two people "cussing" about cricket.

Mr. R. A. THORNE: No. It does not speak about that.

Senator G. P. B. NICHOLLS: No. I am saying that if your interpretation that (b) creates a separate category of offences from (a)….

Mr. R. A. THORNE: It seems that way.

Senator G. P. B. NICHOLLS: Right. Let us go on your assumption and that is so. If I am having a "cuss" out. I like Chanderpaul. You like Hooper and we have a "cuss" out about that, and we are not taking (b) into consideration and I get a hold that somebody recorded a video. "You and Ralph was cussing about cricket". I put this video of me and Ralph Thorne "cussing" about cricket. Right? There is a video about me "cussing" about some cricket years ago and a fellow thought it was funny. Right? I was making some point about Chanderpaul.

Mr. R. A. THORNE: Mr. Chairman, (a) is about….

Mr. CHAIRMAN: Members, can we wait because remember we are still wrapping in an hour's time. Can we wait

until the legal…. Like I said, I regret the legal draftsman is not here.

Senator G. P. B. NICHOLLS: Mr. Chairman, do not stop me on a train because I want to make sure that we understand each other. A person who intentionally uses a computer system to publish a profane….

Mr. R. A. THORNE: Publish data.

Senator G. P. B. NICHOLLS: Publish data which is a video. Let me say it is not pornographic. It is somebody "cussing".

Mr. R. A. THORNE: No. He is not cursing. (a) is a pornographic image.

Senator G. P. B. NICHOLLS: Data.

Mr. R. A. THORNE: (a) deals with images.

Senator G. P. B. NICHOLLS: No, Mr. Thorne. Data can be a video.

Mr. R. A. THORNE: Yes. Of course. A video or a photograph….

Senator G. P. B. NICHOLLS: Right. Let me develop the point. I do not agree with it because it says nothing about speech in (b) to suggest that that is about speech alone. There is

nothing in (b) to determine what would be offensive or what the medium would be. There is no medium described in (b) at all. So, that is why I do not agree with you. So, let us say I published a video of two people cussing about cricket. Somebody would say that that is vulgar, profane and obscene. So, if (b) is not a category….

Mr. R. A. THORNE: How could that be vulgar without **INAUDIBLE**

Senator G. P. B. NICHOLLS: Mr. Thorne, that is why I am saying I do not agree with your categorisation that (b) is separate from (a).

Mr. CHAIRMAN: Members, we are not going to resolve this now. We are going to come back when the draftsman is here.

Senator G. P. B. NICHOLLS: Let me just bring it home. If you publish a video of two people "cussing". Let me read it. A person who intentionally uses a computer system to publish, broadcast or transmit data that is vulgar, profane or obscene is guilty of offence and is liable on summary conviction for a fine of $70,000 or imprisonment of seven years or to both. If the Leader of the Opposition is right that (b) is not a qualification on what goes on in (a), it would mean that if I publish a video of a man "cussing", I am liable to be convicted in prison….

Mr. R. A. THORNE: Under (b).

Senator G. P. B. NICHOLLS: No.

Mr. R. A. THORNE: Not (a). (a) is about images, videos, photographs.

Senator G. P. B. NICHOLLS: You see; he is not…. Leader of the Opposition….

Mr. CHAIRMAN: Members. We are not going to agree. Let us move on because we still…

Senator G. P. B. NICHOLLS: Senator Nurse, you understand the point I am making? Right? I am just saying that you cannot subtract…. He is not speaking law here.

Senator the Hon. L. E. NURSE: I think this is something that cannot be resolved here. I would suggest that we defer it to the draftsman for clarity.

Mr. CHAIRMAN: True. Let us move on, Members. We have only another hour at the most. So, Michelle Bayley, she entitled her written submission, Data, Damage and Liability in the Barbados Cybercrime Bill. She seemed to be concerned that the police did not have enough expertise in the area. She was saying that clauses should be amended to say "in consultation with a qualified cryptologist or computer forensic expert" and "in consultation with a qualified data management specialist", for example, in some of the sections.

I do not know but I mean, that is not normally so in legislation that the police have to have someone who is an expert in fingerprinting to guide them because they have some of that capacity in the police services. So, I was not so sure that her submissions had any merit. You looked at those? We are going through some of them, so we put that one aside. Tell us some more of the substantive ones that we need to consider. Are there any more substantive ones that any Member felt that we should discuss? What about Granville Phillips? Was there anything?

Senator G. P. B. NICHOLLS: Mr. Chairman, for the record, the report would indicate that we received submissions from people and that the clerks will just do a summary of what they submitted? Like a one- paragraph or a one-line? Will that suffice? It would be too invidious of a task for the Committee to sit down here and all five us agree as to what should go into the report from the respective people who submitted from the public because five people's interpretation of what was submitted is not going to cohere into one submission.

Mr. CHAIRMAN: Like I said a lot of them repeat each other, were done jointly and clearly that it is an abridgement of free speech.

Mr. CLERK: Mr. Chairman if the Committee is not going to do that the Clerks will follow what Senator Nichols said earlier where we would say that submissions came in and these are the broad areas that people spoke to because if you are not going to do it that way and the Committee is not going to go through each one individually. It means that the Clerks have to go through each one.

Senator G. P. B. NICHOLLS: I am not even asking you guys to do that. I have read the

submissions and they are about four or five different categories that you can put them in. You are pending the submissions for a report? No. You are?

Mr. CHAIRMAN: The submissions go into the report.

Senator G. P. B. NICHOLLS: Fine take them as read and let us move on. The more important thing here is getting any Amendments to the Bill would be where the focus of the Committee attention in my view should be.

Mr. CHAIRMAN: That is my view too because like I said they were about 50 of them so to try to summarise each of them really and truly does not add up.

Mr. CLERK: Mr. Chairman, just to be clear because the report that was just submitted, the one on Child Justice evidently they did not have 50 submissions.

Mr. CHAIRMAN: They only had 11.

Mr. CLERK: So they went through each one and commented on each one in the report.

Mr. CHAIRMAN: But they only had 11 so I do not know.

Senator G. P. B. NICHOLLS: I move my approach Mr. Chairman that we leave it to the clerks to do a summary of the public submissions. Of course we will pay more particular attention to the institutions that submitted I think in deference to the work that was done that these are the things that were considered by the Committee.

Mr. CHAIRMAN: And that we pick out the areas, the sections and we speak to them. Were they any other submissions that Members feel that we need to go into. As I said we have Mr. Neil Harper's outstanding until the draftsman comes. Do we need a technical person like Mr. Stephen Williams who was a consultant to the earlier Bill to come? No. I agree that we do not need him to come back.

Senator G. P. B. NICHOLLS: Mr. Chairman, I will if the Committee does not mind, I will engage the Minister because I am more fortified in my view that whilst…

Mr. CHAIRMAN: When you say engage the Minister what do you mean?

Senator G. P. B. NICHOLLS: On the issue of whether we need to delineate the specific offences that might fall under the rubric of Cyber Bulling and make them specific offences within the context of the Act because in my view what we have done is that you are going to have the law subject to criticism that something that can be done in person is lawful but something that is when the same thing is done online it now becomes unlawful. You see Cybercrime, they are two aspects to it.

1) Criminal activity that is done online which is already criminal but you are providing now for it to be a crime because it is not being done in person it is being done online.

2) Computer Assisted Crime where you are using the computer to perpetuate a crime and without the computer and the technology the crime could not take place.

There are two different aspects. The way in which we have attempted to define, set up or make provisions. I should not say defined or make provisions for Cyber Bullying conflates those two approaches but it opens up the Section to the criticism that if I were to publish or broadcast indecent material in the newspaper it would not be a crime. That would not be a crime. If I publish photographs and distribute them physically to someone, will that be a crime.

Mr. R. A. THORNE: Yes.

Senator G. P. B. NICHOLLS: No, you are talking about the pornographic element alone but I am talking about again going back to a photograph of someone cussing someone.

Asides

Senator G. P. B. NICHOLLS: I am not getting in that. There is nothing in (b) that says that it is the medium.

Mr. CHAIRMAN: As I said we will deal with that.

Senator G. P. B. NICHOLLS: There is nothing in (b) that says anything that says anything about the medium.

Mr. CHAIRMAN: We will deal with that when the draftsman is here.

Asides

Senator G. P. B. NICHOLLS: But that can be done by video by video too.

Mr. CHAIRMAN: We are not going to solve anything here now. Let us look at because as I said I know that Honourable Peter has to leave at 1 as well. Let us look at Clause 13 because it is similar. Clause 13(2) where they have the words 'and' under receiving and giving of access to computer programme or data. 13(2) "It shall be a defence to a charge brought under Sub-section 1 to prove that the programme or data or access to the programme or data was received in advertently with no intention to commit an offence, was subject to legal privilege and was received by a law enforcement officer in the course of his investigation" I believe that the "and" there should be "or". In other words, it can either be one of those three defences without having to be all three.

Senator G. P. B. NICHOLLS: Again Sir, we cannot resolve that without the draftsman.

Mr. CHAIRMAN: But I mean, would you all agree in principle that any one of those three should be 13(2) on page 15 absolves you from liability. Right. I think it should be or, and then there is the obvious omission in Clause 23(1) where "Judge" should have been included. Search and Seizure. It starts by saying "Where a Judge or Magistrate is satisfied on the information on oath that they are reasonable grounds for suspicion, a crime about to be committed or is being committed to issue the warrant but then it says, "The Magistrate may issue a warrant." so I think that is a clear omission. Line 5 where it only says "The Magistrate may issue the warrant" obviously the Judge or Magistrate I think because it speaks about Judge or Magistrate upfront but then only speaks about Magistrate being able to issue the warrant so I think that the Judge would have to inserted there as well alright. The Bankers Association, I should have mentioned that; they opined that Clause 23(2) provision should be subject to objections to disclosure based on legal privilege, as provided for in the Proceeds Instrumentalities of Crime Act. I just want to draw that to attention; we may not have looked at that Act as yet in detail to see if they have merit in their opinion. It is the third page at the top where Section 23(2)(d) authorises a police officer to have access to any information code technology, which has the capability of transforming or converting an encrypted programme or data. They say that this section should include protection for privileged information or material, as done under the Proceeds and Instrumentalities of Crime Act.

Senator G. P. B. NICHOLLS: That calls for a kind of policy response which I do not think we are necessarily equipped to give. I think these were passed onto the Minister, as I understand it, and I did ask her if she had seen it. I sent it to her but I do not know what the policy of Government is as it relates to that, but I do know that we should strive for some consistency in legislation, which is what you are getting at. Outside of that, I think we may need to have some response from the Minister on that.

Mr. CHAIRMAN: Okay. In the absence of the drafter, does anyone want to raise anything on Section 19? I know we spoke on 20 but we cannot get too far.

Senator G. P. B. NICHOLLS: Without having the draftsman with us, I would want us to defer.

Mr. CHAIRMAN: Sections 19 and 20 fall into similar categories.

Asides.

Mr. CHAIRMAN: Probably write her and ask for a response on that one; the Minister.

Mr. CLERK: What the drafter would say is that those were part of her policy directive.

Senator G. P. B. NICHOLLS: She said that sitting next to me, but we are in a Committee where we are probing, and that is like dealing with opposing counsel where you have a matter in court and they are telling you, "Those are my client's instructions", where the facts demonstrate that there is an issue. The law says how the issue is to be resolved and you are telling them, "This is what my client has instructed me." That instruction is obstructing the progress of the matter, so that if the drafters are going to say, "This is what I was instructed," yes, we know that is what you were instructed because that is what you have reduced to writing in the Bill. However, here it is being pointed out that there is an inconsistency with another piece of legislation where there are facilities of privileged communication between the bank and its customers; under another piece of legislation the banks are only asking for consistency. Therefore, it is outside of the scope of the instructions you

were given only because the policymaker did not consider that. What does that tell you? We know that is what they were instructed but our work here is to ensure that Parliament gets the right Bill. If a matter of consistency of legislation is brought to our attention, you cannot tell me that that is the instruction you were given. That does not make any sense.

Mr. CLERK: That would be a recommendation of the Committee.

Senator G. P. B. NICHOLLS: Exactly, that we should bring into alignment, but if you keep telling me that is what you were drafting then, all right, fine. So if you get foolishness to draft, are you not going to say you cannot do this. As I was taught in Legislative Drafting, laws have to be consistent. You should be able to tell the policymaker this provision is not consistent.

Mr. CHAIRMAN: Right, that is the drafter's duty, to try to bring up consistency in the law. Still, before we go I wanted to see if we can address our minds to one aspect of Clause/Section 19, the malicious communication. At 19(4) there is the word "intimidate". As presently drafted, there is no defence. Intimidation falls into Clause 19(1) and therefore is not defendable by the defences under the Defamation Act. If you intimidate a person, that is that. Then the definition of intimidation in sub-clause 4(a) "to cause in the mind of a reasonable person injury to himself, members of family, dependents… apprehension of violence, damage to person or property…."

Senator G. P. B. NICHOLLS: Can there be any defence to that?

Mr. CHAIRMAN: I agree, there should be no defence to that.

Senator G. P. B. NICHOLLS: Can there be any defence for trying to cause injury to somebody?

Mr. CHAIRMAN: I do not think so.

Senator G. P. B. NICHOLLS: Okay.

Mr. CHAIRMAN: But what about the third limb now? To cause a person substantial emotional distress. Could there, in your opinion, be a defence to that under the Defamation Act's defences? That you intentionally or recklessly use the computer to cause a person substantial emotional distress. Should not that be defendable by you saying that what you are saying is true?

Senator G. P. B. NICHOLLS Mr. Chairman, I suggested that no one should be convicted under that offence if the conduct forms something that serves the public good. That is an offence.

Mr. CHAIRMAN: So you have a similar proposal for Section 20?

Senator G. P. B. NICHOLLS: Yes, no person shall be convicted of an offence under this Section if the conduct that forms the subject matter of the charge serves the public good and does not extend beyond what serves the public good.

Mr. CHAIRMAN: Under that particular limb.

Senator G. P. B. NICHOLLS: As a defence.

Mr. CHAIRMAN: Right, but where you are looking to cause the person violence or damage….

Senator G. P. B. NICHOLLS: The balance is even if it is true, then there may be occasions where I should be permitted to say something that may cause you emotional distress, but I cannot be convicted if the statement I am making is adjudged by the court to be in the public good, and not beyond the extent to which it should be.

Mr. CHAIRMAN: What do other Members think on that point? Any views? Right, so in which case that particular line would have to be taken out and not be part of the definition of intimidate.

Senator G. P. B. NICHOLLS: No, I do not agree Mr. Chairman.

Mr. CHAIRMAN: Do you feel that intimidate should also be defined to mean causing a person substantially emotional distress?

Senator G. P. B. NICHOLLS: Why should it be permitted that somebody should use the computer to publish a malicious communication that causes a substantially emotional distress?

Mr. CHAIRMAN: Even if what they are publishing is true?

Senator G. P. B. NICHOLLS: Mr. Chairman, if I published something that is true, I perhaps watch too much political intrigued dramas on television and things like Blacklist and House of Cards and that kind of stuff, I can get you out of the race by publishing something that is necessarily true and the only way out is by doing harm to yourself. Should I be able to use to manipulate. We are dealing with an era of artificial intelligence where the information that might not necessarily be true but the person does not perceive that it is true, or it can make it look true and the truth is only discern long time after the fact. I will not take it out of that section, because that is saying that I can create and I can use a computer to publish information that intentionally creates emotional distress in someone, and because it might be perceived to be true and when truth cannot be discerned. The truth cannot always be discerning at the moment of the harm being created. In other words, what might be true now might later otherwise found to be false.

Mr. CHAIRMAN: Does any other Member have any other views on that.

Senator G. P. B. NICHOLLS: Mr. Chairman, that is why I said I proffered that alternate that no person shall be convicted if that which is described as criminal conduct serves the public good. The court determines if it served the public good.

Mr. CHAIRMAN: Okay. Are there any other clauses that Members would wish to bring to our attention today? Let me seek to summarise very briefly what we have agreed to have a look at. I do not want to say agreed to in principle, agreed to certainly consider out of what was raised today.

Clause 12 list of critical infrastructure systems that we add to that list. Clause 13, it appears that the word "and" between (b) and (c) should be "or". On the interest of the Bar Association's comments and submissions, we would consider making the offences under Clauses 19 and 20 tribal alternatively, in other words not only by summary trial, but by indictment as well to avoid what the Bar Association considers it seems to be a real possibility of constitutional challenge.

Senator G. P. B. NICHOLLS: Mr Chairman, I do not agree with that.

Mr. CHAIRMAN: I thought that I put that to you and you said that is something that we can consider.

Senator G. P. B. NICHOLLS: Not for the reason that it is unconstitutional.

Mr. CHAIRMAN: Right Okay. Therefore, we admit that part.

Senator G. P. B. NICHOLLS: There is nothing that prevents Parliament from determining an offence is triable in any court. The Constitution is very silent as to that.

Mr. CHAIRMAN: Right, but you agreed that….

Senator G. P. B. NICHOLLS: I just want to reiterate what Lord Diplock said, is that you cannot take away the existing jurisdiction of the court, which you exercised before independence, because the courts are presumed to continue after independence in the way in which they were doing before, but what it cannot do is take away what the High Court had and give it to the Lower Court. However, the Constitution is absolutely silent on that. Therefore, Parliament is free to pass a new law which gives the jurisdiction to magistrates, so it is not unconstitutional. Mr. Weekes is wrong on that.

Mr. CHAIRMAN: Honourable Leader of the Opposition, you were not here when we discussed that. Did you read the Bar Association submission?

Mr. R. A. THORNE: Indistinct.

Mr. CHAIRMAN: Okay.

Senator G. P. B. NICHOLLS:… for the magistrate, therefore unconstitutional.

Asides

Senator G. P. B. NICHOLLS: That is not what Hinds says, because Lord Diplock does

say that Parliament can do whatever it wants to do, and he actually says that.

Asides

Senator G. P. B. NICHOLLS: No, he says that in Hinds, and I am saying that that is a misreading of Hinds. That has been clarified in Suratt.

Asides

Senator G. P. B. NICHOLLS: No, no. he says it can do.

Asides

Senator G. P. B. NICHOLLS: No, no. That is a misteaching or misreading of it for many years. In Suratt, Baroness Hale when the equal opportunities commission was created that argument that "a highly said so" was used. Lord Diplock actually says, Parliament can create any court or tribunal however style. He says that himself. However, what it cannot do is take away the jurisdiction of High Court and give it to a bunch of magistrates.

Asides

Senator G. P. B. NICHOLLS: Yes, but he says, what Parliament can do and then he says what Parliament cannot do.

Asides

Senator G. P. B. NICHOLLS: Yes.

Asides

Senator G. P. B. NICHOLLS: Exactly. We could not take away the power of the High Court. This is not taking away the power of the High Court.

The Committee is saying the Parliament cannot create a jurisdiction for magistrates to determine serious matters and that is unconstitutional.

Asides

Senator G. P. B. NICHOLLS: Create.

Asides

Senator G. P. B. NICHOLLS: That is not so Mr. Thorne. I am going to look for the actual paragraph in Hinds, when Lord Diplock says that Parliament can do so.

Asides

Senator G. P. B. NICHOLLS: I am going to find it now.

Asides

Mr. CHAIRMAN: Sections 19 and 20 are the only two sections that are triable summarily. Is that a concern?

Asides

Mr. CHAIRMAN: When I mentioned the constitutional issue that to just leave it that it could be tried either way. Do any other members have any other views on that? Leader of the Opposition?

Mr. R. A. THORNE: Indistinct.

Mr. CHAIRMAN: Oh. You have not studied it?

Mr. R. A. THORNE: **INAUDIBLE**

Mr. CHAIRMAN: Right. But, is there a proposal to bring in some new rules on this? On trials and all of that? No? Okay. We do not know. Some comments have been made that the penalties are excessive but obviously the penalties are just an upper range, and judicial discretion is there that on conviction, they can fine or imprison way below the proposed penalties. So, I think the feeling was to leave the penalties as they are. Obviously, we are going to have to relook at cyberbullying clause again in the presence of the legal draftsman.

We will examine Mr. Niel Harper's submissions after giving them more thought and in the presence of the legal draftsman. Have I essentially summed up what we have looked at and agreed on in principle for either further consideration or finality today? Obviously, Clause 19, we will look at again because clearly that has to be tightened up as well but in the presence of

the legal draftsman. Okay. Anything else that any other Member wishes to raise?

Okay. Any other business. Alright. So, when can we meet again? The Clerk has indicated the legal draftsman is available on Monday. We do not have Parliament on Tuesday either. Can we agree to meet Monday afternoon and then Tuesday afternoon, and see if we could be near wrapping up?

Mr. CLERK: Not Tuesday.

Mr. CHAIRMAN: What is happening Tuesday, Clerk.

Mr. CLERK: Ms. Hamblin, who is critical to this Committee, cannot make it on Tuesday.

Mr. CHAIRMAN: Which is better? Monday morning, like how we do it now or from afternoon at 2:00 p.m.

Mr. CLERK: I think Senator Nicholls was just saying that Monday morning is bad for him.

Mr. CHAIRMAN: Oh, he said that?

Mr. CLERK: I am certain that is what he said just now.

Mr. CHAIRMAN: Okay. I did not hear him. Okay. So, Monday at 2:00 p.m.? Good.

Mr. CLERK: That is fine.

Mr. CHAIRMAN: Alright. Motion to adjourn.

ADJOURNMENT

On the motion of Mr. P. R. PHILLIPS seconded by SENATOR The Hon. L. E. NURSE, Mr. CHAIRMAN adjourned the Joint Select Standing Committee meeting until Monday, May 27, 2024 at 2:00 p.m. in the Senate Chamber.

6th MEETING
JOINT SELECT COMMITTEE (STANDING)
ON
GOVERNANCE AND POLICY MATTERS
ON THE
CYBERCRIME BILL, 2024
AND THE
MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024

Monday May 27th, 2024

PRESENT:

Mr. Edmund G. HINKSON, S.C., MP, LL.B. (Hons.), L.E.C., LL.M. **(Chairman)**
Dr. Romel O. SPRINGER, J.P., MP., PH.D., (Deputy Chairman)
Mr. Peter R. PHILLIPS, MP
Mr. Ralph A. THORNE, K.C., LL.B., L.E.C., Dip. Theology
Senator The Hon. Lindell E. NURSE, F.C.A, F.C.C.A., R.C.S. (ENT)
Senator Gregory P. B. NICHOLLS, B.Sc. (Hons.), LL.B. (Hons.), LL.M., MCIArb.
Senator Ryan O. WALTERS, M.B.A.

ALSO IN ATTENDANCE:
Mr. Pedro EASTMOND, (Clerk of Parliament)
Ms. BEVERLEY GIBBONS, (Deputy Clerk of Parliament)
Miss Suzanne HAMBLIN, (Journal Department of Parliament)
Ms. Rhea DRAKES, (Office of the Chief Parliamentary Counsel)

ABSENT:

Call to Order
The Chairman called the meeting to order at 2:19 p.m.

Mr. CHAIRMAN: Present are Members of Parliament; Mr. Peter Phillips and Dr. Romel Springer. We have Senator Ryan Walters and we have present Parliamentary Counsel, Ms. Rhea Drakes. We have Senator Gregory Nicholls on via Zoom. He is overseas and has asked to be facilitated in this manner. I just want to be clear, Senator Nicholls, are you hearing us?

Senator G. P. B. NICHOLLS: Yes Sir, I am here.

Mr. CHAIRMAN: Okay, great, welcome. On the agenda for today, we said we would consider the oral presentations and we would have gotten the transcripts over the weekend, the unedited I believe, of the oral presentations. We are going to assume that we have read them and the first I believe we should tackle, is that from Mr. Niel Harper, who would have given written and then presented orally to us as well. We could look at his combined submissions.

I made some notes on his oral submissions, in which we would have expanded a bit on his written and he presented orally on the screen and Parliament also gave us those submissions.

He seemed to be saying that Clause five (5), the Section on modification of programmes or data, is misaligned. It is not present in the Budapest Convention; on the Commonwealth model of cybercrime or in any other cybercrime modelled laws. It is his contention that it is an outdated term and uses outdated language. It also is an unnecessary Section and should be removed.

What are Committee Members' feelings on his submission? Ms. Drakes, obviously we would have you guide and as I said, I am glad to have you here today. We missed you last week and we left open some questions and issues because of your absence which we would deal with today. Do any Members have any views on the Section or what Mr. Harper has submitted?

Senator G. P. B. NICHOLLS: Mr. Chairman, could I ask you through the Parliamentary Counsel, to explain what is the legislative intent on this Section? I believe in Mr. Harper's written submission to us, he left out some key words that are present in the Bill. I do not know if that was an era or that was intentional. What I just wanted to ascertain first of all what is the legislative intent, accepting that this is not the provision that falls within the Budapest Convention.

Mr. CHAIRMAN: Sorry, we lost you there a bit Senator; your last words.

Senator G. P. B. NICHOLLS: Because it is not accepting his ……

Mr. CHAIRMAN: The Budapest Convention, sorry.

Senator G. P. B. NICHOLLS: Yes, the Budapest Convention, accepting that that is his submission.

Mr. CHAIRMAN: For example, he is saying that in these Sections, including Clause five (5), should really focus on someone who is intentionally and without authority causing harm. Ms. Drakes, could you assist us in this regard?

Ms. RHEA DRAKES: Yes, thank you very much, Mr. Chairman for your question and query. Firstly, I would just like bring to the Committee's attention, the fact that Clause five (5) is basically what is in the existing law which is found at Section 3(4) and (5).

Senator G. P. B. NICHOLLS: Is this Section three (3), four (4) and five (5) of the Computer Misuse Act?

Ms. RHEA DRAKES: The Computer Misuse Act Cap. 124B, Section 3(3), (4) and (5), which speaks to modification. It is literally just redrafted in a different format. Instead of having, for example, an interpretation section that had multiple subsections, this new Bill creates a separate section and basically contains all the information in the existing law.

The second point I would just like to make, is that the draft was prepared with the experts of the Council of Europe and that is basically the organisation that is responsible for the Budapest Convention and there were no issues in terms of the provisions and what they seek to do.

Senator G. P. B. NICHOLLS: The inclusion of this, though not a provision within the Budapest Convention, does not necessarily run afoul of the whole schematic.

Ms. RHEA DRAKES: That is correct. It does not run afoul of anything in the Budapest Convention. This is literally the existing law and all that was done, instead of doing a separate amendment, we have a repeal and a replace and those subsections are now found in Clause five (5).

Senator G. P. B. NICHOLLS: This is basically a part of Clause Three (3) that is **recreated in this new section?**

Ms. RHEA DRAKES: Sorry, can you please repeat?

Senator G. P. B. NICHOLLS: I take it that the harm element that he is suggesting is not what the intent here is because if I break into your home with the intent to see what the layout of your security is and how the rooms are but I do not intend to cause harm, that is also a crime.

In other words, Mr. Harper is saying that it should only be a crime when the person causes harm. I understand that to be his submission; where a person is in your computer system, modifying programmes or data and not causing any harm; that should not be an offence. That is what I get him to be saying.

Ms. RHEA DRAKES: Right. Well, the provisions of the Budapest Convention basically speak to intentionally doing something which is the *mens rea*. You must have intended to commit a particular act. The Budapest Convention is not particularly concerned with the effect thereafter.

Senator G. P. B. NICHOLLS: Without authority, is the only then standard of culpability necessary to ground and anchor this offence? Intentionally or recklessly is the *mens rea*; the mental element of the criminal person. Without authority is the only part therefore that anchors the *actus reus*.

Ms. RHEA DRAKES: That is correct.

Senator G. P. B. NICHOLLS: That is sufficient? That you went to someone's computer system to modify their programmes or their data without their authority?

Ms. RHEA DRAKES: Yes.

Senator G. P. B. NICHOLLS: It is not a trick question Ms. Drakes; I just want to be very clear that that is what is the legislative intent of the section. Thank you, Mr. Chairman.

Mr. CHAIRMAN: Ms. Drakes, essentially, you are saying that the Budapest Convention does not identify harm as a consequence for the offence to have been committed? It is just to have the *mens rea*; the

intention and recklessness without authority to ground the alleged offence. That is correct?

Ms. RHEA DRAKES: Yes. That is correct. For example, if we took a provision, let us say child pornography, that speaks to a person who intentionally or recklessly publishes child pornography through a computer system. Now in terms of speaking about the harm, in a case like this; the law does not require the child to have even known that pornographic material about him or herself was present. The effect on the victim is not a consideration. It may be relevant when it comes to sentencing but for the purpose of creating the offence, the Budapest Convention requires, for example, the *mens rea* and *actus reus* of the perpetrator.

Mr. CHAIRMAN: This is just for the record to acknowledge the presence, while Senator Nicholls was speaking, of the Honourable Leader of the Opposition.

Senator G. P. B. NICHOLLS: Mr. Chairman, through you again to Ms. Drakes, looking at Mr. Harper's comments. He is suggesting not only a misalignment with the Budapest Convention and the Commonwealth model law on Cybercrime and other matters but that this section seeks to criminalise modern uses of software and data processing.

When you are downloading programmes, they modify data when you are downloading and none of us are computer savvy to know the extent of the modifications that they make to our computer systems. So, things like downloading software; data processing; when you are using artificial intelligence (AI), for example, and free open sold software, this unduly falls within the wide ambit of this section.

That is his criticism. I know that is not necessarily or it does not appear to me that is the intent of the provision. What balance can we achieve here if that is the case?

Mr. CHAIRMAN: Ms. Drakes, you could assist us with that? The query.

Senator G. P. B. NICHOLLS: He cites AI free and open source software; open data policies; creative commons; data mining and that kind of stuff. So, when you download something your programmes are being modified by some external agency without you clicking or anything. Is it assumed that once you download something, you have given it permission or authority? Is that covered or do you have to expressly state that you are authorising this modification?

Ms. RHEA DRAKES: Thank you for your question. I think that the law is pretty clear. If you look at Clause two (2) or we can go back to 4 or 5. In all the cases, the person who is accessing this information or using the computer system must have acted without authority. If you have the authority to do it; whether it is an employer, somebody who has engaged your services, if you have permission from the application developer or whichever organization or institute it is that you are dealing with, that is fine. It is only where you do not have the authority to access it that that is when the law actually or the commission of the offence kicks in.

The law is not going to penalise you by just using material whether it be software. It is only if you do not have the authority or the requisite permission to access, to modify, *et cetera*.

Senator G. P. B. NICHOLLS: So, you are satisfied that Clause 2(5) which speaks to any modification referred to in subsection four (4), is without authority if the person whose act causes the modification; knows he is not entitled to determine whether the modification should be made and has not obtained the consent of the person who is entitled to the modification.

Ms. RHEA DRAKES: That is correct.

Senator G. P. B. NICHOLLS: That implicit in the downloading of software applications and going into AI and those things start to do their internal harmonisation. I am not a technical person but that is just my language and I start to sync your systems; that permission is there implicit? That would not run afoul of the legislation, as is covered in this subsection (5).

Ms. RHEA DRAKES: That is correct. Those provisions clearly state that a person who intentionally or recklessly and without authority, so you must have access, consent or permission, if you are going to do so lawfully. If not, that is where we have the issue.

Senator G. P. B. NICHOLLS: Okay. So, playing devil's advocate, it would not be too hard a task for someone to say that if you download a programme that I am offering you on the internet and we need to sync our systems, the authority is implicit in your agreeing to download the system. That would not be a hard defence to sell. Correct?

Ms. RHEA DRAKES: Okay. So, authority or permission can come in different forms. If I can give an example from the top of my head, let us say you went to a particular site

and something pops up. They ask you to read this long agreement and you will see a little check box at the end that says, "I agree or I consent" based on I have read all of the rules and agree to the terms. That is your authority there. Once you have agreed to it, you are bound to whatever obligations and terms the developer and the software provider has provided.

That is the other thing too that I want to point out with legislation. We can never draft so narrowly that it captures persons it was not intended to capture.

Senator G. P. B. NICHOLLS: Okay. Thanks, Mr. Chairman. That is it for me. I understand the legislative intent behind the section and do not necessarily agree with Mr. Harper's comments that he makes on that part in Clause five (5) of the Bill which deals with modification of programmes and data.

Mr. CHAIRMAN: I want to just for the record say that we now have present as well, Senator the Honourable Nurse with us. So, we are looking at Clause five (5) and examining it within the context of Mr. Niel Harper's critical comments. Any other Members have other views on this? Mr. Harper uses the same argument with effect to Clause seven (7); Interfering with a computer system. Clause eight (8). Let us say Clause seven (7) first.

Senator G. P. B. NICHOLLS: Mr. Chairman, he also makes comments on Clause six (6). Are you skipping that or are you coming back to it?

Mr. CHAIRMAN: Yes. Clause six (6) as well, sorry. Interfering with data to better align with the Budapest Convention. He says it should be changed. Again, he says it should focus on someone who causes serious harm.

Senator G. P. B. NICHOLLS: He is focusing on whether or not it causes serious harm or not. In other words, you can go into somebody's system without their permission or authority and as long as it does not cause any serious harm; you should not be punished. That is his position with Clause six (6).

Mr. CHAIRMAN: Right. So, Ms. Drakes, what is your response to that?

Senator G. P. B. NICHOLLS: Mr. Chairman, Clauses six (6) and seven (7), he has a common complaint if you look at all three (3); five (5), six (6) and seven (7).

Mr. CHAIRMAN: Right. So, I am just trying to see if Ms. Drakes will commit her response on five (5).

Senator G. P. B. NICHOLLS: The difficulty is that she may not have his comments, so she is looking at the legislation that she is familiar with but not seeing the criticism of it, as we are seeing.

Mr. CHAIRMAN: No. I had asked. Did you get his submissions?

Ms. RHEA DRAKES: Yes, Mr. Hinkson.

Mr. CHAIRMAN: I asked her to make sure that they were sent to…

Ms. RHEA DRAKES: If I could just respond to that criticism now Clauses six (6), seven (7) and eight (8). I would respectfully disagree with the comment that they do not align with the Budapest Convention. I have the Convention in front of me and it clearly provides; if I can Mr. Chairman, if I can just read a couple of the articles if that is okay. Article four (4) for example speaks to data into France:

1) "each party shall adopt such legislative and other measures as maybe necessary to establish as criminal offences under its domestic law when committed intentionally the damaging, deletion, deterioration, alteration or suppression of computer data without right."

If I can just quickly look at system into France, similar language is used where the State has to adopt and establish as criminal offences when committed intentionally and they go on to talk about the Act which is hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deterioration, altering or supressing computer data.

Now, I will start with Clause (6)(1) which provides: *"a person who intentionally or recklessly and it goes onto say and without authority."* So in terms of the Budapest Convention, those requirements have been fulfilled and if you look at Paragraphs A through H, it goes on to tell you the different types of Acts. For example, if you copy or move programme of data. If you destroy, damage, suppress, add, delete or alter.

So again, if we look at Clause seven (7), a similar thing obtains where a person has to intentionally or recklessly and without authority.

If you have authority to do any of those things you are clear. The issue comes where a person does not have the authority. The other thing I wanted to touch on is the fact that these provisions were subjected to quite a lot of scrutiny by the experts again, the Council of Europe and they gave this support for these provisions.

Mr. CHAIRMAN: Ms. Drakes, the question has been raised by some as to the word "recklessly" and we just want you to give your response on the record because the words recklessly are omitted from some clauses but included in others so the words "are recklessly" are omitted from, there are included in Clause four (4), Illegal Access; Clause five (5), Modification a Programme or Data; Clause six (6), Interfering with programme or Data; Clause seven (7), Interfering with the Computer System, Clause nine (9), Misuse of Devices; Clause 11, Disclosure of Access Code; Clause 13, Receiving or Giving of Access to Computer Programmes or Data; Clause 16, Child Pornography; Clause 17, Child Grooming; Clause 18, Online Child Sexual Abuse and Clause 19, Malicious Communication but it is not included in Clause eight (8). Is there a rationale for that?

Ms. RHEA DRAKES: Thank you for your question, Mr. Chairman. My response would be, part of it is mostly policy and if you look at the Computer Misuse Act Cap. 124(B) and I will just choose a section, for example.

Section 13(1) which is the existing law provides:

"a person who, a) publishes child pornography through a computer system is guilty of an offence.

Section 9, for example, has a similar wording where it reads, *"a person who knowingly uses a computer any function."*

Section 10 reads, *"a person who knowingly and without authority discloses any password."*

When we look at for example, Section eight (8) in the existing law, *"it provides a person who knowingly or recklessly."*

It seems that when the law was drafted both intention in terms of "knowingly and recklessly" were provided in certain provisions so that is basically the law as is. With the Bill some of those provisions are mirrored in terms of the ***mens rea***. That is why you will see for example some include and depending on the nature of the offence, you will see only the word, *"a person who intentionally"* does something as oppose to "intentionally or recklessly". Again, my comment would be part of it is policy which the Office of the Chief Parliamentary Counsel (CPC) does not create or get involved in.

Mr. CHAIRMAN: Okay and my last query on Clause eight (8), Illegal Interception of Data. Mr. Harper saying it should only be criminalised; at least it should not be criminalised if it is in the public domain but if the interception is of a non-public sensitive and strictly confidential nature, disclosing strictly confidential information is only then that it should be criminalised. How would you respond to that or is that in your opinion a matter of policy as well too, Ms. Drakes?

Ms. RHEA DRAKES: Okay I would just like to draw the Committee's attention to Article three (3) which is equivalent provision to Clause eight (8) and if you will just permit me to read the provisions of Article three (3), Illegal Interception:

"*Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the interception without right, made by technical means made by non-public transmissions of computer data to from or within a computer system including electromagnetic emissions from a computer system carrying such computer data."*

If we read Clause eight (8) of the Cybercrime Bill: *"it provides a person who intentionally and without authority undertakes an act to intercept by technical means any non-public transmission to, from or within a computer system including electromagnetic emissions from a computer system carrying computer data is guilty of an offence."*

The wording is more than similar to that of Article three (3) of the Budapest Convention.

Senator G. P. B. NICHOLLS: Again, here his focus is on whether the interception is dishonest or whether the interception causes harm; he feels that the offence should only be classified as such in cases where the State is able to prove that the person perpetrating the offence is dishonest or intended to cause harm or was

reckless as to whether any harm could be caused by their actions. Valid criticism but not enough, in my view, to lower the bar for what we are seeking to protect.

Mr. CHAIRMAN: Any Members have any differing views on Clause eight (8)? If not, Clause nine (9), Misuse of devices. Mr. Niel Harper contends that the Budapest Convention says that the misuse of devices; illegal access interfering with a system should not be criminal where it is authorised testing or protection of the computer system.

Senator Nicholls, we know your views on this already. You have stated them more than once and that in your opinion this is comparable to saying that somebody breaks into your house to show that it is not secure and then tells you, *"I told you your house is not secure."*

Are there any other Members who have views on this which are contrary to how the section is worded or in agreement with Mr. Harper?

Ms. RHEA DRAKES: Mr. Chairman, if I can just add on this point. In relation to Clause nine (9) which speaks to the misuse of devices, I noted, Senator Nicholls' belief that it is tantamount to someone breaking into your house and then telling you what the shortcomings are or the lack of measures are. That is all well and good where again, you have been authorised to do so. If, for example, a cybersecurity expert has been authorised by a bank or some other commercial entity or an insurance company, to go into the system and find out the vulnerabilities therein, you have been authorised or you have been engaged.

Sometimes there are requirements that have to be fulfilled or you may only operate within a sandbox, so you cannot go outside of that and for good reason but in all of the cases, this person must obtain authority or consent permission from that person to do so and this is precisely what the law is seeking to prevent persons from just going into other persons' systems, networks and accessing them without authority.

Senator G. P. B. NICHOLLS: So why not broaden it to say, *"without authority, permission or consent …"*? Just to make sure we have all types of cover that could be necessary. You are trying to protect persons who might be susceptible to these kinds of invasions.

We have seen in law, *"authority, permission or consent"*, the three (3) to me, they flow naturally.

Ms. RHEA DRAKES: Senator Nicholls, you are sounding very muffled. We are not hearing you clearly.

Mr. CHAIRMAN: Suddenly, you are sounding a bit muffled, Senator.

Senator G. P. B. NICHOLLS: I cannot control that. I have not changed the tenor in my voice. I am just suggesting that, in addition to the words authority, we could speak about knowledge, permission and consent. Those words are words that are used regularly by lawyers and in legal documents and drafting, to promote the widest possible formulation of the basis of somebody's acquiescence in the Act that is being complained about or the act and the challenger or the act under review; knowledge, permission and consent and it gives a better elucidation of the varying forms in which human interaction can be because it could be implicit; it could be implied; it could be by conduct; it could be through the course of dealings; it could be expressed but if we do it with your knowledge, permission and consent, those words, to my mind, give a much clearer and broader scope for what it is.

When someone runs afoul of it, you could say well your consent was implied because I used to do this all of the time and you did not have a problem with it. Authority seems to be on a much narrow basis and I would be more comfortable if we were to look at broadening the scope there. It is not lowering the threshold of criminal culpability, in my view, but it adds clarity and it uses language that is well applied in many other instances. I hope that that does not do any violence to the workings under the Convention.

That was my suggestion, that wherever we set up the bar for the criminality or for criminal culpability to be established, on the basis of doing something without authority, we should also broaden it to say *"knowledge, permission and consent"* as well.

Mr. CHAIRMAN: So Senator Nicholls, you are proposing that amendment for which Clauses?

Senator G. P. B. NICHOLLS: As an amendment. All of these sections which are used in term of prohibited conduct, Section four (4); five (5); six (6); seven (7); eight (8); nine (9); 10; 11 and 13; those sections, unless there is some case law, Ms. Drakes, that elaborates and deals with these notes which would come up in the various cases in the Courts, that interprets authority to mean all of those things.

Ms. RHEA DRAKES: In my explanation, I was just using some synonyms but I am happy to give you the clarity. What I would say is, if the Committee wishes, we can always include a definition term without authority and say it includes or it means permission, consent or something along that line, if it will grant further clarity, Senator Nicholls.

Senator G. P. B. NICHOLLS: Yes, in 2(5).

Ms. RHEA DRAKES: So wherever the words *"without authority"* appear, perhaps that definition can capture those words. The other thing I wanted to point out, Mr. Chairman, if you will permit me. Under Clause nine (9), the misuse of devices provision which is equivalent to Article VI of the Budapest Convention. The misuse of devices provision clearly states that:

"a person is intentionally or recklessly and without authority producing, selling, procuring, importing, exporting, et cetera, a device primarily designed or adapted for the purpose of committing an offence."

It is not just getting a device or accessing access codes and passwords; the law is pretty clear. It is for the purpose of committing an offence so to my mind, that then removes the possibility of the argument that there is over criminalisation.

Mr. CHAIRMAN: That, in fact, was the note that I made in response to Mr. Harper's written submission that, in my opinion, his argument will not prevail because that section actually says, *"for the purpose of committing an offence"*. A legitimate purpose would not come within the ambit of this; that was my view but I take your point because, Senator Nicholls, when you were saying *"without permission"* and I felt that that was covered already by *"without authority"*. Ms. Drakes proposed that a definition be included expressly as to what *"without authority"* means.

Senator G. P. B. NICHOLLS: I accept that the draftsperson's suggestion that it is better to take it in the Definition section.

Mr. CHAIRMAN: That sounds reasonable. Dr. Springer, I think you wanted to say something.

Dr. R. O. SPRINGER: I was going to support what Senator Nicholls had said about consent and knowledge. I know sometimes when it comes to authority, it can get a little interesting especially if you are dealing with companies where there are varying levels of authority to be granted at one (1) level but that person may not even have the authority to grant it and may be acting *ultra vires*.

I think that a situation where a person can make a claim that this was done without *"my"* knowledge or permission, as opposed to you having an excuse that maybe Member of Parliament Phillips gave the authority. Then the onus is on him now to see whether he has the right to give that authority. You can shift blame when it comes to authority but when it comes to the person's knowledge or permission, then I guess it depends on that individual if that person has actually given you the "okay" to go ahead to access their data or peer into their systems.

If I do not know, if I have not given you the permission, if it was done without my knowledge and it is my system, I can make a claim. You would not have the excuse that the position of the authority was granted by somebody else who, after investigation, we might discover never really had that authority to give that permission.

I think that in relation to the recommendation by Senator Nicholls – just to rephrase that – even if we put the two (2) together, we should put a definition in there. I think that would give greater clarity. That is what I was going to say earlier before you then intervened and clarified that you too support such an intervention and such an amendment.

Senator G. P. B. NICHOLLS: Mr. Chairman, Dr. Springer, Member of Parliament has made the point better than I could have made it. His example is spot-on.

Mr. CHAIRMAN: Alright. Any other Members wish to express their views on this Clause, Clause nine (9)? If not, Clause 11, Disclosure of Access Code, where Mr. Harper says that this Clause should be removed since it is not treated as a cybercrime in the Malabo Convention; Commonwealth Model on Cybercrime or the Budapest Convention.

Senator G. P. B. NICHOLLS: He is commenting on Section 11? Disclosure of access code? I am not seeing that in his written submissions.

Mr. CHAIRMAN: Let me see if I find it then, because that was the note I made.

Senator G. P. B. NICHOLLS: That may have been in his oral submissions. In his written report he does not make any reference to Clause 11. The one (1) that I have from him goes from Clause seven (7); eight (8); nine (9) to 12. On Clauses 10 and 11 there are no comments. Then he refers to Clauses 12-19, to 23, 24, 26 and 28, so I do not see anything under Clause 11 unless he made that in his oral submissions, and I was not taking notes of what he said at the time. I am not contradicting you, Mr. Chairman but I am just saying that is what I am seeing in front of me.

Mr. CHAIRMAN: What is your opinion? Is his statement correct in the first place?

Ms. RHEA DRAKES: Sorry, can you repeat what his argument or submission was on Clause 11.

Mr. CHAIRMAN: The note I have from his oral submission was that Clause 11, dealing with disclosure of access code, should be removed since it is not treated as a cybercrime in those Conventions, namely Budapest, Malabo which is an African Convention and Commonwealth Model on Cybercrime.

Ms. RHEA DRAKES: Clause 11 of the Cybercrime Bill is basically Section 10 of the Computer Misuse Act which is the law of Barbados. I just want to make a distinction here because Parliament can make laws that can prevent the commission of offences. Now whilst we are not necessarily speaking about a computer system; if we understand the technology and how it moves, I think the Committee can agree that passwords and access codes are fundamental to accessing computer systems.

In those circumstance, I think the policy, it is incidental to committing computer-related offences as well as content-related offences. It is squarely within the Committee's remit if it wishes to take out Section 11 but I see no reason why it should be precluded from the Bill.

Again, the disclosure of the access code must be done intentionally or recklessly and without authority. Cyber offences can be committed where a person who has no authority intentionally discloses a passcode to the computer system. It could be one for a critical infrastructure system.

Senator G. P. B. NICHOLLS: I am not trying to sound ridiculous but could you be prosecuted if you were to give this access code to somebody? Let us say the police asked for it. Can you be prosecuted for giving it to the police because you have no authority to give it to the police. In other words, the recipient of it should not have any authorised access to it. Is that not what you are seeking to criminalise? Not only the person doing it without permission of the owner but giving it to someone who has no authority to receive it as well. I think that is perhaps where you may need to focus. The section states, *"A person who intentionally or recklessly discloses any password, access code or any other means of gaining access to any programme or data held in a computer system to anyone who is not authorised to receive the same, is guilty of an offence."* That is how my mind is working around this here right now.

Ms. RHEA. DRAKES: Senator Nicholls, in relation to your example, whether a person should be penalised or can give it to a police officer. I would think that that information would be pursuant to any court orders or such. I do not think it would applied to any police officer.

Senator G. P. B. NICHOLLS: Suppose an internal auditor of a company or something is doing some special occasion to determine whether is being given for a lawful purpose but the person does not have the authority to receive it. Would that also now be a crime? The offence is created if the person does not have authority to give out the code and the information. If there is a lawful purpose for which that person is giving information which they are not authorised to give out and the person is lawfully entitled to receive that information, would that not be an overreach?

In other words, are we criminalising something that might be useful from a policy perspective?

Ms. RHEA DRAKES: Okay, so two (2) things, Senator Nicholls. Clause 11 speaks to the disclosure of the passwords and the access codes. There is no offence in relation to receiving it under Clause 11. I also want to point out under Part Three (3) of the same Bill, there are provisions where persons may assist police officers and also where ……

Senator G. P. B. NICHOLLS: There are penalties for not assisting police officers. Police officer was the wrong term because there are penalties for not assisting police in terms of being able to get into systems and so forth but I am talking about somebody for example internal audit or somebody who is doing some work within the company and let us say, there are within organisations who do internal investigations and so forth, where their work need not to be disclosed. Whistleblowers or people investigating complaints made by whistleblowers. A person who is authorised to carry out that investigation, might need to access a passcode from an employee or person within the organisation and this is a legitimate aim that is being pursued but that person is not authorised to give that passcode to anyone else without the permission of their superior. Passing it to the internal investigator or auditor, will that be a crime? I know that in that the legislation cannot necessarily solve all the problems in the world that might occur and that is why I always think that prosecutorial guidance and regulations are necessary particularly in legislation like this. That is something that readily comes to mind because I am aware of, particularly in the banking sector how those things are unearthed and discerned and people can get themselves in trouble for passing information to assist in investigations and that has come up in some employment matters to as well. People have gotten fired for things like this as well.

Ms. RHEA DRAKES: I just want to draw the Committee's attention to Part Three (3) of the Bill which provides a procedure for persons who wish to obtain that information; they have to go to a judge or magistrate. That information cannot be given out without that type of authority and if you have the authority of the court now authorising you to provide ……

Senator G. P. B. NICHOLLS: Did you say in Clause three (3)?

Ms. RHEA DRAKES: Part 3.

Senator G. P. B. NICHOLLS: Sorry?

Ms. RHEA DRAKES: In that case then, you will be doing so with right; with the authority.

Mr. CHAIRMAN: Okay, I accept that response. Okay, just for the records, what I took there from Mr. Harper's argument is on page five (5) of the Hansard that we were sent over the weekend, Monday, 06 May, 2024 where he speaks on Clause 11. "At the end of the day this is not treated as a cybercrime in the Malabo Convention and the Commonwealth model on cybercrime, as well as the Budapest Convention. This is not just addressed; I do not see a reason for this Section."

Is there anything else on any submissions written or oral from Mr. Harper that any Member would wish to raise for discussion purposes because the rest of course is tied up in you know Clauses 19 and 20, which we spoke on the last time we met.

If not, we would want to go to Mr. Steven Williams and his oral submission. He gave written submission as well and there were just two (2) issues that I would want to raise. Ms. Drakes, he said the Bill will need regulations, I think that is recognised that they would need regulations for this Bill to become fully operational?

Ms. RHEA DRAKES: Thank you, Mr. Chairman. Clause 30 provides that, *"The Minister may make regulations generally for the purpose of giving effect to this Act."* The enabling provision is present in the Bill. It is the instructing Ministry or for example, if it is the piloting department that would have to provide the policy for us to draft but the framework is there; the power is there for the Minister to do so.

Mr. CHAIRMAN: Right. I think we addressed Mr. Williams' issue a bit earlier on. He queries, for example, whether sharing for example the Netflix password with a third party would specifically lend to a penalty under "Disclosure of access codes", Clause 11. I know it certainly would not come under Clause 11(2).

Senator G. P. B. NICHOLLS: Mr. Chairman, I am not sure about that because the Netflix password is your password. If you share it with somebody, then certainly it would not be an offence if Netflix call the police because that would be a breach of your contract with Netflix that you are not to share your password. I do not think sharing your own password with a third party can claim that it is a crime and elevate a breach of your contract Netflix into a crime, so I do not agree with him.

Mr. CHAIRMAN: Are there any other views on that issue? If not we could move to Mr. Anthony Greene and remember Mr. Greene spoke a lot on freedom of information legislation which is in our remit, although I do agree with him that we should have freedom of information legislation in Barbados.

The issue I would wish to draw to Ms. Drakes, is Clause five (5), where he says in connection with ……..

Senator G. P. B. NICHOLLS: Mr. Chairman, you are moving quickly. Are you going to Mr. Greene and BARJAM?

Mr. CHAIRMAN: Pardon?

Senator G. P. B. NICHOLLS: Are you still at Steven Williams or you have moved onto to Mr. Greene and BARJAM.

Mr. CHAIRMAN: I asked if there were any other views. Did I? If not, let me repeat. Is there anything else Mr. Williams has raised that any Member would wish have for discussion and give their comments and opinion on?

Okay, if not, we move onto Mr. Greene. Like I said, he spoke a lot about Freedom of Information Legislation.

Senator G. P. B. NICHOLLS: Mr. Chairman, sorry to correct you but I think that he came in his personal capacity. He came to us to represent BARJAM (Barbados Association of Journalists & Media Workers).

Mr. CHAIRMAN: Who did you say he came to represent?

Senator G. P. B. NICHOLLS: BARJAM.

Mr. CHAIRMAN: No, I think he said he was representing Starcom Network.

Senator G. P. B. NICHOLLS: Starcom!

Mr. CHAIRMAN: He did not say he was representing BARJAM.

Senator G. P. B. NICHOLLS: Yes. Starcom, sorry.

Mr. CHAIRMAN: Remember we subsequently received a written submission from BARJAM.

Senator G. P. B. NICHOLLS: Just for the record, we do not want to say that it was him in his personal capacity because he was saying that he was representing Starcom Network.

Mr. CHAIRMAN: Right. I think he is the General Manager. Is he not? He is a manager there. A senior manager, for sure. In relation to Clause five (5), Modification of programme or data which prohibits illegal interception of information which is Clause eight (8) and he felt that that should not criminalise journalistic or media publication in the public interest. In other words, there should be an exception for journalistic and media publication in the public interest to that section; Illegal interception of information which is Clause eight (8). Do Members have a view on this?

Ms. Drakes, this would be a policy decision, Right? Or this was up for discussion when the Bill was drafted?

Ms. RHEA DRAKES: In relation to Clause eight (8), I am not sure if you can provide the nexus between the protection of journalist and the illegal interception of data.

Mr. CHAIRMAN: No. Well, what did Mr. Greene say on this? I think he is just trying to have a cover that in the absence of freedom of information legislation, that journalist or the media would not be subject to criminal law for publications in the public interest. Was that issue discussed during the scripting of this Bill?

Ms. RHEA DRAKES: In relation to Clause….

Senator G. P. B. NICHOLLS: I am not seeing that is a legitimate concern.

Mr. CHAIRMAN: Alright. Let us go to his oral evidence.

Senator G. P. B. NICHOLLS: If you could explain what you understand to be his concern, I would be better able to understand.

Mr. CHAIRMAN: No. I want to go to what he actually said because I am not in a position to explain what he said at all. But, I just wanted to raise it for discussion. Let us see where he said this. Page 19? Okay. He says on page 19, *"Even when it is reasonable to sanction those who breach a computer system to obtain information or share information beyond its authorised recipients; journalists should be allowed to receive and report on the information they receive without fear of retaliation. I will add, so long as the journalists or media personnel are acting in the public interest, this is definitely core to work of the media."*

Senator G. P. B. NICHOLLS: So, you are understanding him to be saying that if the media publishes a report that is indicative of the interference of a computer system, that the media should be not charged as an accessory for that crime? That is what you understand him to be dealing with? Right?

Mr. CHAIRMAN: Ms. Drakes.

Ms. RHEA DRAKES: Mr. Chairman, unfortunately, I am not *clear about the concern there.* Clause eight (8) reads, *"A person who intentionally and without authority, undertakes an act to intercept by technical means…."* It does not speak to the publication and the broadcasting of any material….

Senator G. P. B. NICHOLLS: But, if they intercept, Ms. Drakes, in the purpose of the investigation of the story. Suppose, they can access and investigate, the

investigative journalist should have some leeway to investigate and bring things to light.

Ms. RHEA DRAKES: *"an act to intercept by technical means".*

Senator G. P. B. NICHOLLS: This is Section eight (8), right?

Ms. RHEA DRAKES: Yes. Clause eight (8). If you look at the provisions, there is no criminal offence or penalty for receiving or publishing, so I would require greater clarification.

Senator G. P. B. NICHOLLS: Yes. Interception could take place in any form. Correct?

Ms. RHEA DRAKES: By technical means. Yes.

Senator G. P. B. NICHOLLS: Any form. It can take place in any form. So, I can download an application that could allow me to listen in on somebody else's conversation.

Ms. RHEA DRAKES: Sorry. Senator Nicholls, can you….

Mr. CHAIRMAN: This section is repeated from the Computer Misuse Act?

Senator G. P. B. NICHOLLS: No. I am just saying that this section is not intended to criminalise that activity but it can fall within that activity, where any who is investigating anything; whether it be a journalist or a personal investigator (PI). For me, if there is a public interest in the interception, it should not be a crime. In other words, there should be a public interest defence to Section nine (9).

Mr. CHAIRMAN: Did that issue come up for discussion, Ms. Drakes?

Ms. RHEA DRAKES: Not that I recall, Mr. Chairman.

Mr. CHAIRMAN: What do other Members feel? You are saying, Senator Nicholls, your view is that there should be a public interest defence only for the journalist and media? Senator Nicholls? Honourable Leader of the Opposition, what do you think? We have lost Senator Nicholls, it seems.

Senator G. P. B. NICHOLLS: Mr. Chairman, you have not lost me. I am very much here.

Mr. CHAIRMAN: Yes. Sorry, you are back. Your view is that the public interest defence should only be for the journalists and media?

Senator G. P. B. NICHOLLS: No. I am saying that there should be a public interest defence here because there may be people who are conducting surveillance. You would not want if there is a legitimate public interest which can be adjudged by the courts to be so, that the person would not be able to avail themselves of that as a defence to this crime. So, this is not something that the drafter would be able to assist us with. It is a policy issue here.

Mr. CHAIRMAN: Exactly.

Senator G. P. B. NICHOLLS: But, I can well see if journalists get a scoop that something is about to go down and the only way you can prove that this is so is if you put a tap. A tap is something that would otherwise be illegal that we would appreciate. We do not have any laws dealing with in this intersection of communication generally in Barbados but this would be a situation where, since the Computer Misuse Act but before that, there was none in terms of telecommunications. I do not know; I am not a technocrat but the point I am making is if there is a legitimate public interest in it and one is able to establish the **bonafide** of that legitimate public interest, I would question hearing whether or not we should no allowed for that defence to come up.

Mr. CHAIRMAN: And only for this particular Clause?

Senator G. P. B. NICHOLLS: Not necessarily for this particular Clause, Mr. Chairman. Not only for this particular Clause. I can see this working in relation to malicious communication as well. A person should not be convicted under the Act if the conduct forms what is the public interest or serves the public good.

Mr. CHAIRMAN: No, so for which Clauses you feel such a defence should extend to eight (8); 19, Malicious Communication. Which other ones?

Senator G. P. B. NICHOLLS: Mr. Chairman, I think that we cannot conceive of all the situations now and I think that it should be a general defence. The Court is who will adjudge whether your actions are in the public interest or constitute a public good. That is determined by the court and the court is also going to determine whether you have met the evidential threshold to say that I have had enough evidence to suggest that this is an issue that would allow, say, if this was to go to a jury for the jury to determine whether if it was fact that you had. That is why and now I am thinking that if you had a public interest **defence** here; it would buttress that protection that people have that legitimate and lawful activities in the interest of the public might be necessarily and unduly caught in a wide net. This is not necessarily a defence to go to a particular section but just a general defence in relation to anything within the Act.

Mr. CHAIRMAN: Ms. Drakes, what is your view?

Ms. RHEA DRAKES: Thank you, Chairman. I just had a couple of questions for clarity. When Senator Nicholls was speaking several things were raised. As it stands now Clause eight (8) speaks to a person who intentionally and without authority undertakes an act to intercept by technical means, so my question would be what type of act are we speaking about?

Senator G. P. B. NICHOLLS: Just like you said, Rhea, we cannot define it or locate it with any specificity here because the legislation here because the legislation is drafted in a broad and general way.

Ms. RHEA DRAKES: The reason I ask is because the section goes onto say, *"from or within a computer system."* It is specific to computer system so what type of act just by way of example would….

Senator G. P. B. NICHOLLS: If John Brown had child pornography or John Brown had child pornography on his system and he is accused of teaching little girls Maths lessons at St. Leonards' Girls School and he is collecting this and a parent for example, says to a friend who is a journalist, "Look, I got my suspicions about this man." The journalist goes and talk to the computer whiz guy at the Barbados Investigator and he says, *"Man, look I got a programme that I download hey. If I can just get an email and stuff like that, we can see whether he got dis ting on hey."* The investigative journalist and the tech

guy goes into John Brown's computer to discern that this is so. Is that a crime?

Ms. RHEA DRAKES: The reason I ask and your example Subsection two (2) of Clause 16 already speaks to that where you have the defences in relation to those types of situations. If is bonafide, research, medical, law enforcement purpose but my question is and it goes back to in what circumstances would a person undertake an act to intercept by technical means from or within a computer system?

Also raised in your earlier statements were the receipt of the information by the journalist as well as broadcasting and publishing. If it is the Committee's recommendation based on its consideration of everything that we were discussing here to provide a separate subsection that would give journalists some sort of defence but in terms of a narrowing scope but I cannot see the removal of Clause eight (8).

Senator G. P. B. NICHOLLS: No, I am not talking about the removal of Clause eight (8). I am just saying that there should be a general public interest defence. We cannot now conceive of all of the things that could be done in breach of Subsection in Clause eight (8) when it becomes law that would be within the public interest but by virtue of not having a public interest defence, none of the public interest elements could be played in aid of, if someone were charged under that Act not necessarily intending to do harm but intending to serve some public and legitimate interest. That is my concern. It is more a policy point in our drafting.

Mr. CHAIRMAN: Senator Nurse, I have not heard you today yet. What is your view? I was asking Senator Nurse if he had a view.

Senator the Hon. L. E. NURSE: I feel that when we refer to intention, it should a broad thing available not only for the media but it should be as broad and as wide as possible because I think that anyone can use not necessarily and not doing something intentional but it can happen and we need to have a very broad interpretation so that those people who may do something but not necessarily doing it with the intent of malice or doing it illegally; doing some improper thing that they should also have some level of protection.

Senator G. P. B. NICHOLLS: In other words, is the section intended to protect criminals from detection by anybody? Journalists; members of the public; people sitting down behind a computer all day looking for Cyber criminals? We are talking about a changing world and dynamics; people in the gay economy. We are not only talking about a static environment of the past, so I am just saying why not allow a public interest defence?

Mr. CHAIRMAN: Dr. Springer, you have any view on this. No comment. Minister of Parliament Phillips, you have a view? The same. Okay. Ms. Drakes, could we agree that you draft an exception which can encompass this, knowing that we are just a recommendatory committee?

Ms. RHEA DRAKES: Okay, Mr. Chairman and this will be limited to just public interest?

Mr. CHAIRMAN: As opposed to what?

Ms. RHEA DRAKES: The media or …

Senator G. P. B. NICHOLLS: We are not limiting its application to any particular group or targeting any particular group because once you start to include some you would exclude others by necessary implications. Anybody acting within the public interest where that public interest could be identified and that is a question for the Court to determine; not for somebody just to allege it and the police to say, *"Alright, yes, I understand."*

The intent would be to have this as a public interest determined by the Court. It is done in Canada and in other places where these are proper defences to any of these types of computer infractions. I would daresay that if the public interest defence were not included in it and somebody who was legitimately active within the public interest and so demonstrate; then you would find that the section might find itself challenged, if somebody were to invoke the public interest defence was, let us say, constitutionally clear.

The over-broad nature of the offence would have to be necessarily curtailed by the Court or if we cannot curtail it, it would have to strike it altogether and then you would find yourself without the offence that would be protecting persons' interests. Then you would have to come back and redraft it but if you put in the public interests' element here, the proportionality of that

incursion of one's rights is balanced out with the public interest element here.

Mr. CHAIRMAN: So, Ms. Drakes would draft an exception for our consideration. Is there anything else on anything Mr. Green said? If not, can we move on to Ms. Janine Butcher? What I took out as her concern and the one (1) I would want to engage Members on, there is the need to protect whistleblowers who may be disclosing information in the public interest but again, what we just spoke of would cover that, to prevent the law from being used against individuals seeking to expose corruption or misconduct. What we have asked Ms. Drakes to look at a to draft would cover that as well. Unless there is anything else from Ms. Butcher.

Mr. Timón Howard, what I have taken out from his submissions was that he submitted that licence to be given for artistic commentary and that should be allowed in legislation provisions so that criminal sanction does not attach to artistic commentary.

Again, would the public interest issue, Senator Nicholls, in your opinion, cover Mr. Howard's concern?

Senator G. P. B. NICHOLLS: Mr. Chairman, I understand that you and I might feel that it would but remember sometimes the public interest is determined by who is sitting down in the courtroom at the particular time. It is not something that is objectively determined; it is determined from what a case-to-case basis. So that, my good schoolmate, Dyestra Browne, he does his thing online and stuff like that. I would like to think so, that it covers it but there might be some people who might interpret that very strictly and not include the artistic license enjoyed by spoken word artists; cartoonists and other people who might peddle their trade online.

The Honourable Leader of the Opposition spoke about the culture of the calypsonian in Kaiso Review and Calypso Spectacular and in those places, Demarche Gras Show. Wayne "Watchman" Hade and Michael Anthony "Sugar Aloes" Osouna and those men going far beyond where we would go in Barbados. I have seen it and heard it with my own ears but that is the accepted standard there.

Mr. CHAIRMAN: Do any other Members have any views on whether some carving out for artistic commentary should be made? This is considering that you would have the defences already.

Senator G. P. B. NICHOLLS: Mr. Chairman, I think that the best thing for this to be done at the policy level is for the prosecutorial guidelines which would have to be issued.

Mr. CHAIRMAN: I am going to mention that.

Senator G. P. B. NICHOLLS: That is one (1), I think, that you would have to issue a prosecutorial guideline on. Where the State would say it would have no interest in prosecuting people who are performing artistically and that kind of stuff and their performances are recorded and transmitted online for the purposes of a crime under this Act. That would have to be a guideline because there might be some performance. If you watch a Chris Rock on Netflix, clearly what he said about Will Smith and Jada is defamatory.

Maybe under his contract, if he gets sued Netflix selling all over the world would be able to pay out some money and would be settled, I do not know but certainly our laws do not allow people say those kinds of things about other people. I do not know what is the statute law of the United States of America (USA) on that kind of thing but certainly I sit down and watched Netflix; that thing that Chris Rock did and it was funny; it was very interesting but certainly, it went beyond **the opinion of law in many different** regards.

Some people might think what he said about gay people, Chinese and Indians are obscene and intending to cause them embarrassment and interfere with them and that kind of stuff but some might be thinking that is just Chris Rock, a comedian.

Mr. CHAIRMAN: Okay. Before I come to the guidelines, is there anything else from any of the other oral presentations that we would want to discuss? Taking into account that Minister Caddle obviously brought her proposed amendments to Sections 19 and 20 into account and we discussed those the last time we met.

Okay. If not, I need your guidance here, Mr. Clerk of Parliament. We have Guyana and we have Jamaica; The Caribbean Community(CARICOM) countries that have

similar legislation. I saw, Ms. Drakes, that you mentioned that Belize has this legislation as well?

Ms. RHEA DRAKES: That is correct.

Mr. CHAIRMAN: Alright. Is it similar within the same ambit?

Ms. RHEA DRAKES: Similar provisions, framework and offences.

Mr. CHAIRMAN: Okay, I will look at that. Within our Report, Mr. Eastmond, can we attach these pieces of legislation in relation to Guyana, Jamaica and Belize, as the three (3) CARICOM countries with cybercrime legislation? Can they be attached as guides within our Report?

Mr. CLERK: If you are going to refer to them and it depends on what is the purpose of attaching them.

Mr. CHAIRMAN: Okay, right, as I said I have not looked at these but I think we mentioned Jamaica and Guyana a lot and you may want to draw comparisons within the Report on certain sections. You are saying that once comparisons are being drawn to any of the sections, that we can include them in the Report?

Mr. CLERK: Do you want to include the entire book or do you want to make reference to the particular sections?

Mr. CHAIRMAN: The particular sections that we draw reference to and include those. Okay. The Belize Act, Ms. Drakes is saying is from 2020?

Ms. RHEA DRAKES: That is correct.

Mr. CHAIRMAN: Right, so they are the only three (3) CARICOM countries that have legislation on cybercrime updated to your knowledge?

Senator G. P. B. NICHOLLS: Did the British Virgin Islands or Bermuda did not pass legislation last week or the week before?

Mr. CHAIRMAN: Remember Bermuda is not in CARICOM.

Senator G. P. B. NICHOLLS: That is not the point. They are a Commonwealth Caribbean country. They share the same constitutional structure as we do, same and except that they are British Overseas Territories but in terms of the fundamental rights and provisions of their Constitution, they are still the same.

You see cases from Bermuda and the Bermuda court reporting cases in the West Indian Law Reports. I would not exclude it just because they are CARICOM countries.

Mr. CHAIRMAN: Have you been able to download their whole Act because all I was seeing was on one (1) section where they had a heavy penalty on an aspect which is not covered by our Bill as presently drafted. Were you able to see their whole Act?

Senator G. P. B. NICHOLLS: No, I have not seen it. I saw a press release that they had passed legislation dealing with cybercrime; that was what I saw.

Mr. CLERK: Mr. Chairman, we will reach out to the Clerk of the Parliament in Bermuda and see if we can get the Act.

Senator G.P.B. NICHOLLS: It is either Bermuda or the British Virgin Islands. I am not sure which one (1), sorry.

Mr. CHAIRMAN: It was Bermuda, yes. Is the Belize one (1) on the internet, Ms. Drakes?

Ms. RHEA DRAKES: Yes, they are all available online.

Mr. CHAIRMAN: Okay. Then there is the issue, as Senator Nicholls mentioned, about guidelines for prosecuting cases under this Bill; involving malicious communications. Jamaica has done some guidelines, so again, Mr. Eastmond, it would be if we referenced that, it would attach any aspect of that to the Report.

Mr. CLERK: When we are going through the files, you can make reference because they would come under regulations.

Senator G. B. P. NICHOLLS: No, those are not regulations that are made by the Minister, Pedro. Those are prosecutorial guidelines issued by the State prosecuting authority. This is what we are looking at to prosecute in this country from the prosecutorial standpoint. That discretion is given and I only discovered this last night; speaking to a colleague of mine in Guyana that it is not an independent discretion in every Caribbean country, whereas the Director of Public Prosecution (DPP) has an independent

prosecutorial authority vested by the Constitution of Barbados. That is not so in some countries in the Organisation of Eastern Caribbean States (OECS), where the Attorney General's Office can still issue directions as to how the prosecution should be conducted. Certainly, this is different and distinct from the Minister who speaks to regulations that govern the broad policy framework of the legislation and its operations; its enactment and its enforcement.

When it comes to prosecutorial discretion, the prosecutorial authorities in the countries under the Budapest Convention do issue guidance, so that members of the public can appreciate and understand clearly what conduct is prohibited and what is acceptable; what conduct would be such that would pique the attention of the prosecution's services and the police in their investigations. Conduct that would ordinarily be unlawful but not necessarily be conduct that would be intercepted and prosecuted with the vigour of other offences. That is the prosecutorial discretion. Nobody can force the Director of Public Prosecution to bring a prosecution under this legislation if the DPP does not think that a prosecution is necessary or warranted in the circumstances.

Certainly, citizens can bring private prosecutions, as is the situation with all criminal sanctions, but that is not the same thing as the Ministerial regulations that operate the legislation; that is something different. As I said, it is something that occurs under the Convention countries, or countries that are signatory to the Convention. We do not have that culture of the prosecutorial directions in Barbados but this is a new piece of legislation and we are dealing with something as pervasive as technology and the internet and I think it is right for that entry into the legal infrastructure here in Barbados.

Mr. CHAIRMAN: We should attach these guidelines as a guide for that. Ms. Drakes, what I am interested in hearing your response on is this: We have had a Computer Misuse Act for 19 years, almost two (2) decades. Certainly some of the earlier provisions or clauses in this Cybercrime Bill as presently drafted are repeated from the Computer Misuse Act. Are you aware of any prosecutions under the Computer Misuse Act, under those clauses?

Mr. CLERK: Mr. Chairman, just to be clear, where are we on the Agenda?

Mr. CHAIRMAN: As I said, are we finished with oral submissions? Remember I asked that. Is there any Member who would wish to raise any other issues under any of the other oral submissions? If not, let us go on to Item three (3): Consideration of the Bills. I was suggesting that some of the clauses, certainly in Part two (2) of the Cybercrime Bill as presently drafted, are repeated in principle from the Computer Misuse Act. The proposed penalties are greater but repeated and I was asking Ms. Drakes if she knows of any prosecutions.

Mr. CLERK: How are we approaching the consideration of the Bills? Are we just doing them generally?

Mr. CHAIRMAN: I am going to ask Members again for their input, so, Ms. Drakes?

Ms. RHEA DRAKES: Thank you, Mr. Chairman. Off the top of my head, I cannot recall in any of the meetings that I would have attended, where reference was made to any particular prosecutions. I suspect that the more appropriate authority may be the DPP's Office or the police. Thank you.

Mr. CHAIRMAN: Okay. Consideration of the Bills. Members, I think we have spent a lot of time with the written and oral submissions. I think we got close to 50 written submissions and 11 oral; people who came before us and presented. Have we addressed our minds to these Bills and what we would consider as amendments to these Bills?

I just wanted to say, with the Bankers' Association, they gave written submission because we had some questions for you, Mr. Drakes from last week. I think one (1) was with the Bankers where they too felt that the Cybercrime Bill should include protection for privileged information or material as it is done they say under Proceeds and Instrumentalities of Crime Act. Your response was that that was a policy decision that would have to be made, right?

Ms. RHEA DRAKES: That is correct.

Mr. CHAIRMAN: Their concern is over Section 23(2)(d), where,

"A warrant issued under this section may authorise a police officer to have access to any information, code or technology which has the

capability of transforming or converting an encrypted programme or data held in or available to the computer system into readable comprehensible format or text, for the purpose of investigating any offence."

They seem to feel that should not have to apply to them for privileged information.

The reality was that Banks have to disclose in certain circumstances, so I do not know that that particular argument would carry much weight. Are there any views by Members on that? Now, Ms. Drakes had said that that has to be a policy decision but I know we raised this issue a bit last time we met. Have we addressed our minds further to it to give an opinion?

Mr. CLERK: Mr. Chairman, I hear the argument of policy decision. Now, this Bill is in this Committee before the second reading stage, which is usually the stage where policy is discussed. I do not think the Committee could say to Ms. Drakes, go and amend the section based on a recommendation as a policy but certainly, the committee can make a recommendation as a policy because remember when the report is done; the report goes back to the House of which it was originated and that House then has to debate and adopt, reject any suggestions or amendments proposed by the Committee.

Ms. Drakes cannot act on those recommendations because she is the drafter but certainly the recommendation could be in the report, as to thing that hinge or touch and concern policy. As I said, it cannot be reduced into an amendment because it is ultimately up to the Government which makes the policy but certainly the Committee could make the recommendation.

Mr. CHAIRMAN*:* We accept that. Has anyone studied the Bankers' concerns or would want to make an input on it? What I would ask is certainly for our next meeting, to let us address our minds on that issue to see if you want to agree with the Bankers as well on that.

Mr. Eastmond, do you remember the other issues we had for Ms. Drakes or have we covered all of them from last week?

Mr. CLERK: The emails you introduced, I think you would have covered all of them. If we have missed any, Ms. Drakes will be with us for the duration of this Committee.

Mr. CHAIRMAN: Senator Nicholls, correct me if I am wrong. Mr. Drakes, had raised the issue of a definition of cyberbullying in Clause 20. He cited Canadian Legislation Criminal Code 1985 on that issue.

Senator Nicholls, you had said you were going to do a bit more research on it. Did you have that opportunity as yet?

Senator G. P. B. NICHOLLS: Yes, Mr. Chairman. It seems to me that cyberbullying itself is not defined in the legislation of any country as is specific crime but it is more recognised as a class in which certain crimes could occur with the use of technology. When we look at the Canadian example which was cited at the last meeting and I am sure everyone has the minutes now. You will see that those individual offences are carved out as specific offences and not necessarily within the context of any computer or cybercrime legislation but just generally.

I was wondering whether or not we were trying to create an omnibus legal construct that might be too large to give the necessary clarity and precision where it is necessary. That is why we have so much general and unbridled language within Section 20 and giving people cause or concern of words that will not necessarily be criminal, if we did them in our day-to-day lives but because it is on the computer, might give people some cause for concern and we know that those words are.

Annoyance, if they annoy you by playing music that is not a crime but if I cause inconvenience that is not a crime; if I cause embarrassment that is not a crime. Humiliation and intimidation, that is not a crime. We are importing this broad language into it constructed legal concept of cyberbullying, when in fact there are specific aspects of cyber bullying, such as revenge porn; using threats and intimidating language and that kind of stuff to cause people to alter their course of conduct and ordering behaviour to coerce people into doing things that they would not otherwise do.

Those are specific instances of cyberbullying but if we use this method here, I am

fearing that it will create more problems than are necessary. I think that that is my only challenge with the Section. I would prefer if he were to identify what are the elements in cyberbullying that are the target of the drafter and spell them out as individual offences rather than having a broad class and then using very broad and vague language to determine what is actually a crime or not. That is my only criticism of it.

I do believe that cyberbullying should be addressed in the legislation but perhaps if we were to narrow it down as the Canadians do. If I may be permitted to share my screen, perhaps that might be… can you all see my screen? In Canada, cyberbullying can be against the law. Right. If you go down here, these are the criminal charges that come under Canada's criminal code. They are as follows:

- Sharing intimate images without consent
- Criminal harassment
- Uttering threats
- Intimidation
- Mischief in relation to data
- Unauthorised computer use
- Identity theft
- Extortion
- False messages
- Indecent and harassing phone calls
- Counselling suicide
- Incitement of hatred
- Defamatory libel
- Public incitement of hatred offence against the person and reputation
- Offence against the person and reputation

These are the possible charges that could come under the broad ambit of cyberbullying. Each one (1) of them is defined in a particular way. So that, for me, I do not have a diametrical opposition to Section 20, as is stated but I understand why persons might be necessarily apprehensive in having conduct associated with some of the words here which may not necessarily be a crime if we were not using a computer; would now be a crime because we are trying to target isolated and specific instances of harm, that you could see from the list but are not necessarily coming out to you if you look at Section 20 of our Act. That is just my concern. If you want me, I can stop sharing the screen now.

Mr. CHAIRMAN: Senator Nicholls, you are going to send what you just shared to us?

Senator G. P. B. NICHOLLS: Yes. I can send it but I mean, it is up on the internet. Sorry. I mean, it is up on the internet. I got it from the Government of Canada official website. So, that is where I got it from.

Mr. CHAIRMAN: What is your view, Ms. Drakes.

Ms. RHEA DRAKES: Mr. Chairman, I just wanted to quickly go back to the comment in relation to privileged information and if it is possible to ascertain precisely which provisions in the Proceeds and Instrumentalities of Crime Act that the association wishes the Committee to consider for inclusion.

Mr. CHAIRMAN: When I looked at the Act, the only ones I could possibly think they were relating to, I think, it was Section 154 or 155?

Ms. RHEA DRAKES: Right. Section 154 (10) reads,

"A search and seizure warrant does not confer the right to seize privileged material."

There are other provisions in there at, I believe, Sections 151, 33, 133(2)(i), 41 and 145 which speaks to unexplained wealth and disclosure orders. Just a narrowing down of the provisions for consideration.

Mr. CHAIRMAN: For consistency, would you agree that cybercrime should also treat to it that way as well, if it is in a previous piece of legislation?

Ms. RHEA DRAKES: As a drafter, yes, depending on the nature of the material; there can be references or portions of provisions that are replicated in other pieces of legislation. As to

their inclusion and the effect thereof, that would not necessarily be something we would do without further instructions from the piloting Ministry.

Mr. CHAIRMAN: Alright. Secondly, now the issue of what Senator Nicholls has raised with defining cyberbullying.

Ms. RHEA DRAKES: Yes. In relation to the legislation referenced by Senator Nicholls, depending on the jurisdiction and the existing laws that they have, in some cases there is, as Senator Nicholls referenced, various offences that can fall within the ambit or scope of what can be considered or maybe considered cyberbullying.

In other jurisdictions, cyberbullying is defined otherwise. So, for example, in going back to what Senator Nicholls had up on the screen, if you had seven (7) enactments with various pieces or types of offences, they are not all found in one (1) place, in terms of drafting style, what Senator Nicholls showed me, exists.

In other cases, the legislature there would have formulated their own definition, offence or specific offence. In relation specifically now to Clause 20 of the cyberbullying, it is my understanding that the bullying which is what was trying to be captured, it appears in various forms. Bullying is really the offensive behaviour; the nature of the behaviour that is what we are trying to crimimalise. As I said, it can come in a particular provision or as Senator Nicholls showed us just now, various pieces of our enactments may have offences that can be deemed or considered as cyberbullying.

Mr. CHAIRMAN: What would be your preference as a drafter? How the section is drafted at present or to specify certain actions?

Ms. RHEA DRAKES: Thank you for your question. Our Cybercrime Bill contains several offences which align with the Budapest Convention and others that are included to generally protect society. For example, there would be provisions in there that may address revenge pornography or malicious communications. In a case like that, it may be prudent perhaps to keep cyberbullying. I believe on the last occasion I was here, the Minister made certain recommendations for the Committee's consideration in terms of the deletion of certain words. I do not see Clause 20 as one (1) that should necessarily be removed. I think it can remain and we can make the necessary amendments to it, based on the recommendations that were made.

Senator G. P. B. NICHOLLS: Ms. Drakes, the drafting style that was used in subsection one (1) is the subject of debate, even within this Committee. Is it your understanding that Clause 20(1)(a) and (b) are two separate offences or that (b) is a qualification on the conduct that is unlawful in (a)?

Ms. RHEA DRAKES: Thank you for your question. I would answer in the affirmative. It is more or less a qualification. They are not two (2) separate offences.

Senator G. P. B. NICHOLLS: It is not clear to say that one (1) speaks to words and the other speaks to data, although there is no reference to data in sub-clause (b)? But, you would not agree that that is the interpretation that youu would give? that (a) speaks to words and (b) speaks to data; two (2) separate offences.

Ms. RHEA DRAKES: Right, so there are not two (2) separate offences as you pointed out. Paragraph (a) speaks to the acts that are committed. For example, publishing, broadcasting, transmitting, that type of material and in relation to (b), it speaks to the effect.

Mr. CHAIRMAN: That was my reading of it as well and you would recall that when one (1) of the oral presenters. I cannot remember which one (1), was treating it as two (2) separate. I told him that as far as I can read and my interpretation of the law, that it (b) qualified (a).

Senator G. P. B. NICHOLLS: would it help Mr. Chairman, if we were to remove (b) and to bring that out so that it would read, *"A person who intentionally causes a computer system"*, so take out (b) altogether? When I say take it out, I mean, not to take out the words that follow (b); take out the letter (b) in brackets.

Mr. CHAIRMAN: At the end of (a).

Senator G. P. B. NICHOLLS: At the end of where the semicolon, sent, *"to be so sent; for the purpose of causing, annoyance, inconvenience, danger, obstruction,*

embarrassment, insult, injury, humiliation, intimidation hatred anxiety or causes substantial emotional distress to that person is guilty of an offence and is liable on summary conviction to a fine of $70,000 for a term of seven (7) years or both. What is as (b) is read as conclusion of 21(a).

Ms. RHEA DRAKES: My recommendation for the Committee's consideration would be to remove paragraphs (a) and (b) and just have one (1) sentence so that it flows.

Mr. CHAIRMAN: That can work.

Ms. RHEA DRAKES: In addition to the deletion of the words that the Minister had recommended.

Mr. CHAIRMAN: Okay. There was also 13(2), *"receiving, giving access to computer programme or data"* and we are thinking that instead of the word "and" there, it should be "or". At (b), 13(2) between (b) and (c). It shall be defence to a charge brought under subsection one (1), to prove that the programme data or access was any one (1) of those three (3), not all three (3), so it should be "or" instead of "and".

Senator G. P. B. NICHOLLS: Or take out the word "and" altogether Mr. Chairman because if you put "or" there, you would wonder why not "or" after "a" and only after (b).

Mr. CHAIRMAN: How about the drafting because this seems to me to be all separate; how in drafting would you do that Ms. Drakes? You would have to put an "or" at the end of (a) and "or" at the end of (b) as well?

Ms. RHEA DRAKES: No, I believe at one (1) of the earlier sessions or meetings, the recommendation was made in relation to Clause 13(2) to substitute "and" at the end of paragraph (b) was the word "or".

Mr. CHAIRMAN: So you would not have to put "or" at the end of paragraph?

Ms. RHEA DRAKES: No. The "or" would come before the final paragraph.

Mr. CHAIRMAN: Okay, great. Members, do you all recall any other issues we had said last week that we would raise with Ms. Drakes? I do not recall that there was anything else. Members, what I think we should do here now is to go through each Clause and I will try to summarise what I glean from it. Well, I am going to ask are there concerns with this Clause? We would raise the concerns; what seems to be the view in the absence of contrary views expressed here on each Clause and then it would be a question of and I would take responsibility as Chairman, trying to define what are the proposed amendments ad to have them sent to all the Members, to add; subtract; modify; amend and that we come back here then with the Parliamentary Counsel, Ms. Drakes to discuss the proposed amendments.

14 June, 2024 will soon be here; so can we agree on that approach to go through each Clause now and just I mean, for the sake of the record. Point out if we have an issue with them and what the issue is. If we do not, we say that. Okay. Clause one (1) obviously is good. Clause two (2) are there any issues with any of the definitions?

Dr. R. O. SPRINGER: I was asking, you said we were going to include a definition for authority?

Mr. CHAIRMAN: Ms. Drakes, the definitions we spoke about would come here at the front because I noticed in Clause 19 for instance, you have definition. Not you, there is a definition of intimidation, no intimidate within Clause 19 and as well injury; so how do you choose to have definitions there within the Clause as opposed to upfront in Clause two (2)?

Ms. RHEA DRAKES: My recommendation would be to include a definition for "without authority" in the Interpretation Section or Clause Number two (2) and this would be 2(1) because it is used frequently throughout the provisions of the Bill.

Mr. CHAIRMAN: But you have or rather, the definition for intimidate and the definition for injury are only by Clause 19 because they only pertain to those.

Ms. RHEA DRAKES: That is right.

Mr. CHAIRMAN: Although injury is also used in 20. The word injury is used in 20 as well, so you would still have to extend the definition of injury in my opinion, for it to cover the word injury as it is in Clause 22.

Ms. RHEA DRAKES: In relation to 19(4); those two (2) terms well; I believe I reference

earlier in both Guyana and Belize that the style is consistent where a section or once we are using a particular subsection, a subsequent or subsection will provide clarity in relation to that. If it is that you wish to remove injury from the definition section of (b) of sub-section four (4), it can be removed. What I would also say is that sometimes…

Mr. CHAIRMAN: It could be removed and put in Clause two (2).

Ms. RHEA DRAKES: Yes. If it appears more than once. Yes, the other thing is in terms of drafting style, you may have a word that is defined in a particular subsection or it has a specific meaning in that subsection; so you may not always want to place it for example, in the Clause two (2).

Mr. CHAIRMAN: Sorry, can you repeat that?

Ms. RHEA DRAKES: In terms of drafting, there are words that may be used and have a specific meaning within that particular provision, so that they would stay in that section to which they relate because they may have, for example, a more limiting or narrowing scope as opposed to if you use it in its ordinary meaning.

Mr. CHAIRMAN: Is the definition or the use of the word injury in Clause 19 the same as it is in the Cyberbullying Section Clause 20?

Ms. RHEA DRAKES: I would say, based on my reading, it could have the same meaning. The only other thing I would add is that I am seeing a note from one of the previous meetings where the term "reputational injury" was preferred in Subsection four (4) of Clause 19. If it is that we are talking specifically, reputational injury as opposed to general injury, then I am guided by the Committee.

Mr. CHAIRMAN: I remember we did say "reputational injury" for Clause 19, whereas Clause 20, just "injury" can suffice.

Ms. RHEA DRAKES: Yes.

Mr. CHAIRMAN: The word "injury" in Clause 20 then would not need a definition?

Ms. RHEA DRAKES: It would be used as …

Mr. CHAIRMAN: As its plain and natural meaning. Alright. For Clause two (2) and as I said, what I want to do at least from my understanding because in the absence of any objections or contrary opinions or comments, alright. We add, "without authority" to that definition in that Section and based on what we said, Ms. Drakes, would reputational injury would only then be used in Clause 19? Would that then remain defined in Clause 19 and not in Clause two (2)?

Ms. Rhea DRAKES: That is correct.

Mr. CHAIRMAN: Okay. Any further comments or possible amendments to Clause two (2)?

Clause 3: Application.

(1) It says this Act applies to an Act done or omission made,

a) in Barbados, that is, in the territory of Barbados, b) on a ship or aircraft registered in Barbados. Again, a ship or aircraft registered in Barbados has implications in terms of the jurisdiction is registered in Barbados or

c) by a national of Barbados outside the territory of Barbados. If the person's conduct would also constitute an offense under the law of a country where the offence was committed.

In other words, where there is an offence under this Act, committed or alleged or alleged committed by a national of Barbados outside of the defined territory of Barbados. In other words, for example, in the United States of America (USA); Canada; England or Europe, if that alleged offence or the person's conduct constituting that alleged offence would be an offence as well in that country outside of the territory of Barbados that this Act applies to that national of Barbados.

In other words, countries that would have similar cybercrime legislation with similar offences as constituted in this Act, this Act would capture that national of Barbados even though they are outside of Barbados. Is that the correct understanding, Ms. Drakes?

Ms. RHEA DRAKES: Yes, that is correct, Mr. Chairman and it is also Section two (2) of the existing Computer Misuse Act.

Mr. CHAIRMAN: Obviously, with the mutual assistance in Crime Amendment Act which we are also looking at here, you would be able to request assistance in prosecuting that person. Is that correct?

Ms. RHEA DRAKES: That is correct.

Mr. CHAIRMAN: Okay. Are there any proposed changes to that Section or that Clause by anyone?

If none, let us go on to Clause four (4). Senator Nicholls, your proposal is here because you said that from Clause four (4) down to number 11, I think, all of them you want to propose …

Senator G. P. B. NICHOLLS: Mr. Chairman, I accepted the advice of the drafter that the appropriate section dealing with "without authority" could be put into the definition section to include where that language is used in the Act; that it could also refer to without the person's knowledge, permission or consent rather than having to insert all of them into the sections. I think that was what she recommended as a drafting tool and that solves my query.

Mr. CHAIRMAN: So in other words, you would not have "about the public interests" that you were raising but just the …

Senator G. P. B. NICHOLLS: No. I thought you were speaking about the whole question on "without authority". I am sorry. My apologies.

Mr. CHAIRMAN: Right. That is "without authority". Yes, and we dealt with what that would be but in addition, your public interest defence would …

Senator G. P. B. NICHOLLS: For any offence in Part II of the Act, I believe it is Part II. Let me just make sure that I … Not Part II because …

Asides

Senator G. P. B. NICHOLLS: Mr. Chairman, did I mention public interest in relation to Clause four (4)? I do not think so.

Mr. CHAIRMAN: No. You did for Part II but what I am saying is, for Clause 14, "Computer related forgery", I do not see how you could have any defence in public interest for that.

Ms. RHEA DRAKES: It was Clause eight (8), Mr. Chairman.

Mr. CHAIRMAN: So only Clause eight (8)?

Senator G. P. B. NICHOLLS: For me, I am just looking at it here now. That would be Clause four (4); five (5); six (6); seven (7); eight (8) and nine (9).

Mr. CHAIRMAN: So, Clauses four (4) to nine (9) inclusive?

Senator G. P. B. NICHOLLS: Yes, hold a minute. Clauses four (4) to 11 with the exception of 10 and then also applicable to Section 19.

Mr. CHAIRMAN: No but in Section 19 you already have defences so I would not agree to that. You already have Section 19(5) defence, so I do not think you would need to include public interest in there.

Senator G. P. B. NICHOLLS: Okay, fair enough. Clause four (4) to 11 with the exception of Section 10. It deals with access with intent to commit a further offence.

Mr. CHAIRMAN: So it is Clause four (4) to 11 excluding 10. Is that right?

Senator G. P. B. NICHOLLS: Mr. Chairman, let me come back to that because my submission this afternoon was not in relation to Section four (4) or any of these things and I want to be careful by not putting something before the Committee that was not my intent and just going along in the summary. I did not address Section four (4). I did not address my mind to it.

Mr. CHAIRMAN: So you want to limit it to eight (8)?

Senator G. P. B. NICHOLLS: No, I am going through it now, Mr. Chairman.

Mr. CHAIRMAN: Ms. Drakes, you are saying if we put this in, this is a bit contrary to the Budapest Convention? Rather, if we make this recommendation.

Ms. RHEA DRAKES: Mr. Chairman, what I was saying is that I do not wish to get into too much detail in relation to my earliest submissions but Clause eight (8), which speaks to legal interception of data, "intercept" is defined in Clause 2(1) as follows: *"In relation to a computer*

system, listening to, monitoring or surveillance or recording of function of a computer system or acquiring the substance meaning or purport of the function."

My question then and still is, under what circumstances would a person intentionally and without authority undertake an act of interception by technical means from within a computer system? If it is that the thinking was to protect journalists or persons who wish to receive information or broadcast or publish information that they have received; it is up to the Committee to decide what sort of protection it would give to those persons; whether it be public interest for investigative or enforcement purposes. That is something the Committee can make a decision on.

Mr. CHAIRMAN: Senator Nicholls?

Senator G. P. B. NICHOLLS: Yes, Mr. Chairman.

Mr. CHAIRMAN: What say you then with that explanation or clarification?

Senator G. P. B. NICHOLLS: It does not change my view, Mr. Chairman. I am standing by the fact that these interactions with computer systems and data; where a person can establish that their actions can be justified as protecting the interest of the public, they otherwise should not be criminalised as a general defence.

Mr. CHAIRMAN: On whose burden of proof would this be?

Senator G. P. B. NICHOLLS: The burden of proof?

Mr. CHAIRMAN: Yes, to prove that they are acting in the public's interest.

Senator G.P.B. NICHOLLS: The burden is an evidential burden, not a legal burden. Any defence is always an evidential burden. In Canada, it says *"no person shall be convicted of an offence under this Section, if the conduct that forms the subject matter of the charge serves the public interest and does not extend beyond what serves the public interest."* That is in one (1) of the offences in Canada that deals with cybercrime.

Mr. CHAIRMAN: Like I said, you will send that to us.

Senator G. P. B. NICHOLLS: It also says that for the purposes of that Section, it is a question of law whether the conduct serves the public interest and whether there is evidence that the conduct goes beyond what serves the public interest. It is a question of fact whether the conduct itself does or does not extend beyond what serves the public interest, so the legislation sets a legal standard. If there is a jury trial, the judge would determine whether the conduct serves the public good and whether there is evidence that would be tantamount to establish that fact but the question of fact would remain for the jury. I should say "a question of fact" which is different from "a question of law". That guidance is given directly from the next section without any qualification at all.

Mr. CHAIRMAN: There are some sections where naturally, automatically committing the act would not be serving the public interest and that would be in instances where there is critical information infrastructure system, Section 12 or computer-related forgery, Section 14 or computer-related fraud, Section 15.

Senator G. P. B. NICHOLLS: I would not go beyond Section 11 but certainly Sections four (4) to 11 with the exception of Section 10.

Mr. CHAIRMAN: Okay. Ms. Drakes?

Senator G. P. B. NICHOLLS: It is not for Ms. Drakes. I think it is the Clerk saying that she is not here to draft things for us. She is to give us guidance on how it was drafted and what is the legislative intention and the drafting instructions. If we agree to adopt it, we can adopt it as a recommendation and the House is free to say 'yea' or 'nay'.

Mr. CHAIRMAN: Are you comfortable with that, Ms. Drakes?

Ms. RHEA DRAKES: Yes, Sir.

Mr. CHAIRMAN: In terms of the penalties now between Section four (4) and 11, are we ……..

Senator G. P. B. NICHOLLS: Mr. Chairman, we discussed that last week.

Mr. CHAIRMAN: Are there any Sections ……

Senator G. P. B. NICHOLLS: Mr. Chairman, did we not discuss that last week?

Mr. CHAIRMAN: Pardon?

Senator G. P. B. NICHOLLS: Mr. Chairman, did we not discuss the penalties last week?

Mr. CHAIRMAN: Yes, but we are going through the Sections again with Ms. Drakes here. Are there any Sections where we want to propose an adjustment of the penalty between Section four (4) and 11? Last week there were none.

Senator G. P. B. NICHOLLS: That is why I was asking, because there was no proposal.

Mr. CHAIRMAN: Like I said, we are going through and we are giving everybody the opportunity to make an input if they wish.

Section 12, critical information infrastructure system. Ms. Drakes, what we said last week, is that we would want to expand this. This is too narrow even though yes, it could be amended by publication in the **Official Gazette.** We know practically these things could take a little time with everything else a Ministry is doing, so that we would suggest some additions and we had them and like I said, when I prepared the amendments for discussion, proposed amendments we would have them there for you. We included things like hospitals; law courts; public utilities; I think transportation; whereas this lists seems to be limited in Clause 12(1).

Ms. RHEA DRAKES: Mr. Chairman, I would say that Clause 12 is a significant improvement from the existing Section 11? One (1) of the observations was that as you rightly pointed out, sometimes it may take long time for changes to be made to the list. In fact, when you look at CAP. 124 there were no amendments in the almost 20 years that it has been around.

Mr. CHAIRMAN: They have a similar section in the Computer Misuse Act?

Ms. RHEA DRAKES: Yes, in terms of protecting what is called restricted computer systems of Section 11 of Cap. 124. It was mainly set out in the Schedule and then the Schedule would be amended by order as necessary.

With Clause 12(1)(g), that is what we call a catch-all because there are so many different areas, that you may not necessarily be able to list everything; it is an inexhaustible list. That is why it is worded, *"any computer system, programme or data that maybe designated as a critical information infrastructure system"* and it goes on to say, *"that is so vital that the incapacity of destruction of such computer system, programme or data would have a debilitating impact on the security, national economic security, national public health,"* which will cover things like medical institutions, hospitals, *et cetera "or safety or any combination of those in Barbados."*

Mr. CHAIRMAN: Yes, all of that is good language but it is only when it is published in **Official Gazette** that it applies.

Ms. RHEA DRAKES: No, that last part which reads, "*that is so vital that the incapacity of its destruction that would include any type of computer system"*, that would include any type of system that may affect those areas or sectors.

Mr. CHAIRMAN: Sorry, go over that again, Ms. Drakes.

Ms. RHEA DRAKES: Which part Mr. Chairman?

Mr. CHAIRMAN: For example, you are saying functions that relates to let us say Government services that is so vital.

Ms. RHEA DRAKES: Okay, so Clause 12 (1), provides or gives an idea of the types of systems that are being referenced here. (a) to (f) for example, provides a list of electricity, telecommunication, government services, which can be anything basically, emergency services, *et cetera*.

Then at the bottom you will see, which is the following paragraph, *"that is so vital that the incapacity or destruction of such computer system would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters in Barbados,"* so that this line or that paragraph is not only connected to (g) it is all of the paragraphs.

Mr. CHAIRMAN: Hospitals for instance, even though it is not specifically mentioned would come within.

Ms. RHEA DRAKES: Yes, that type of system.

Mr. CHAIRMAN: It is vital to national public health. Okay, so you are then saying that we do not really have to add to that list.

Ms. RHEA DRAKES: I am saying that the list is much approved from what is currently the law. If the Committee is minded to make recommendations to include or specify in greater detail other types of agencies or sectors, that is completely within the remit of the Committee.

Mr. CHAIRMAN: You do not think it is necessary because of that?

Ms. RHEA DRAKES: Well, that section was intentionally drafted with a very broad language to encapsulate anything that may be best, but for sure anything related to finance, mentioned the court systems, and that type of thing it would fall within the existing Clause 12.

Mr. CHAIRMAN: Financial and insurance services is one (1) that would come within that.

Ms. RHEA DRAKES: Yes, that is correct.

Mr. CHAIRMAN: Okay, there is no need to add as you have explained it. Are there any thoughts or comments on Section 13? We talked about changing the "and" to "or". Are there any comments of Section 14? Are there any comments of Section 15? Are there any comments of Section 16, Child pornography?

Ms. Drakes, corporations, I think I raised this issue with Sir David Simmons. Corporations are only liable in this Bill as presently drafted under child pornography, child grooming and online child sexual abuse. Is there any reason for that? Is it that it is going to be asking corporations to do too much and it is going to be too much of a burden on them, for corporations to be liable under the earlier sections of Part 2?

Ms. RHEA DRAKES: Thank you for your question. Under the Interpretation Act, Cap. 1 of Barbados, a person includes a body corporate which would be a company. The reason company or corporation was specifically referenced in those two (2) provisions you referenced was for the purpose of distinguishing the fines just to make it higher. In all legislation, where you see a person that includes both a natural person who is an individual, as well as a company or body corporate.

Mr. CHAIRMAN: Right. It is because the fines are higher in each of these sections for a corporation that they specifically said corporation. Okay. Anything on Clause 17 or 18? Clause 19? We have been through to take out some of the words. As I said, I would propose some amendments and bring it to the Committee Members for discussion as to whether you feel these are the words that are taken out; whether we should take out more than what we have and also taking into account what the Minister had proposed to be taken out.

We could agree to take out more than what she proposed. Alright. Clause 20. Ms. Drakes, we agreed on how we would try and clear up this ambiguity because there was disagreement at the last meeting and that is among attorneys-at-law of seniority. So, we cannot have a clause drafted where people who are not trained in law can clearly be confused. So, we said we will take out (a) and (b). Right?

Ms. RHEA DRAKES: Yes.

Mr. CHAIRMAN: Have it as one (1) straight clause? Obviously take out some of the words. Cyberterrorism. Any issues with that clause? Alright. Clause 22; Aiding or abetting. Any issues? Alright. Part III; Search and Seizure. Clause 23(1), I think we had agreed that the judge should go in there as well in line five (5).

Ms. RHEA DRAKES: Yes.

Mr. CHAIRMAN: Any comments in relation to the rest of Clause 23? We are going to have a look, Ms. Drakes, as we said, with these Proceeds and Instrumentalities of Crime Act to see if consistency with this Act means that you have to give an exemption there for privileged information. Right?

Ms. RHEA DRAKES: Yes.

Mr. CHAIRMAN: Okay. Sorry. Before we go on to Part III, Ms. Drakes, you read the Bar Association's comments written by Mr. Brian Weekes? He is saying that Sections 19 and 20

should be before a judge, as opposed to a magistrate. He says that these offences carry heavy fines or jail terms. They are not minor offences. A magistrate does not have the security of independence or tenure, as a judge.

Under *Hinds* vs *The Crown*, in Jamaica, that was a gun court issue that they should be tried where the Privy Council said that those offences should be tried by judges and not magistrates; where the Gun Court Act purported to have gun-related firearm charges before, I think, it was a panel of three (3) resident magistrates.

What we were discussing last week was that we would make Sections 19 and 20 alternative charges. In other words, is liable on summary conviction or indictment. In other words, giving the accused the choice whether to be tried before a magistrate or a judge. They are the only two (2) offences that, as the Bill is presently drafted, are triable on summary. That is correct. Right, Ms. Drakes. All of the others are triable on indictment. I think it was said that the reason for that is because before the magistrate, the case would be heard and tried quicker than before the judge. Was there a discussion on this earlier on?

Senator G. P. B. NICHOLLS: Mr. Chairman, are you sure that somebody said that that is the reason?

Mr. CHAIRMAN: I have heard so much. It may have not been before this Committee. That is my understanding. So, yes, let me….

Senator G. P. B. NICHOLLS: That is as flimsy a reason to distinguish why these two (2) offences are summary and the others is ….

Mr. CHAIRMAN: So, let me ask, Ms. Drakes. Was this discussed during the meetings in crafting the Bill? Why those two (2) sections are summary and they are the only two.

Ms. RHEA DRAKES: Mr. Chairman,….

Senator G. P. B. NICHOLLS: Mr. Chairman, before Ms. Drakes answers your question, can I also ask her to couple it with answering this question? Is there any policy justification to your mind, for these two (2) offences in Clauses 19 and 20 to be tried summarily, whereas the other offences are to be tried on indictment only?

Ms. RHEA DRAKES: In relation to Clauses 19 and 20 and the offences therein, I cannot recall now any conversations that may have taken place surrounding those two provisions, Senator Nicholls.

Senator G. P. B. NICHOLLS: The other $70,000 offences and $50,000 offences are triable on indictment. Right. For example, Illegal access is triable on indictment; $50,000 or five (5) years. On the **modification** of data, $70,000 or seven (7) years. Interfering with data; $70,000 or seven (7) years. Interfering with a computer system, similar. Illegal interception of data $100,000, 10 years so it seems as that the increments of $10,000 per year is warranted here. Refusal of data $70,000 or seven (7) years. Access to information is similar. Disability of access codes similar. Provision of critical information infrastructure system $100,000, 10 years and then it could go up to 150 and 12 so that is the only variation where the $10,000 per year is not apposite.

Thirteen (13) goes back to 70,000 on indictment or seven (7) years; computer related forgery 100,000, 10 years; computer related fraud same thing. Child pornography well this is a little different. This is on indictment again $100,000, 10 years; a corporation is larger fine. Child grooming, same thing as in child pornography. Online sexual child abuse is $100,000 similar things but malicious communication is done at the level of a magistrate but it maintains not the minimum fine but a $70,000 fine and cyberbullying is the same thing.

Section four (4), I believe; not 4. There is one that is a $50, 000 fine. Section four (4) is illegal access is on indictment and you would think that illegal access is not as serious a crime as cyberbullying but that is a $50, 000 fine on indictment and cyberbullying is a $70,000 fine, summary conviction and I cannot discern a policy justification or any consistency where it relates to why these crimes are triable summarily.

Mr. CHAIRMAN: Ms. Drakes, you said that this did not come up; this was not pointed out in the earlier meetings?

Ms. RHEA DRAKES: No. I am saying I cannot recall because this Bill would have been drafted over a period of maybe two (2) or three (3) years and they were different meetings at different points. I cannot recall; but I am not saying that there is not but at this moment I cannot recall.

Mr. CHAIRMAN: I discern the view as I said there was the intention that these offences could come before a Magistrate and be tried quicker than before a Judge but there is no consistency.

Senator G. P. B. NICHOLLS: Mr. Chairman, that is on par with the Barbados Bar Association's view.

Mr. CHAIRMAN: Pardon?

Senator G. P. B. NICHOLLS: The Barbados Bar Association's view is that should not be carried before a magistrate at all.

Ms. RHEA DRAKES: What I would suggest then, if further clarity is necessary from a policy decision; perhaps we can seek assistance or guidance from the Law Reform Commission.

Mr. CHAIRMAN: I have spoken with Sir David Simmons on it and I am of the view too as well as you but that is off the record there, that we can make them where the accused has the choice and there is legislation like that. You are liable on summary conviction to X and liable on indictment to Y and you are given the choice. Do you want to be tried before the magistrate or the judge? The magistrate now to reduce, I would propose reducing the fine and sentence to $50,000 or five (5) years on summary but on indictment leaving it at $70,000 or seven (7) years.

Senator G. P. B. NICHOLLS: Mr. Chairman, I got a lot of problems with what you just said and I do not want to repeat what you said last week because if the accused elects and he elects summarily, then a matter is serious or treated as serious in a court where a fine of $60 000 is given for the same offence, is now up to the accused person whether or not he wants to face the judge and that kind of stuff.

I do not think that we should be just willy-nilly or without any juridical or jurisprudential or philosophical basis be making an adjustment to a policy decision that comes under the legislation to reduce fines just for the sake of saying we are reducing fines. If we accept the Barbados Bar Association's criticism which I do not agree with.

To put a crime or to create an offence where a fine is $60,000 or $70,000 and have it at the discretion of the magistrate is unconstitutional; ties of the Queen does not say that. We are not taking away any existing jurisdiction of a judge and give it to a person who is not appointed with the security and tenure, a High Court judge. That is not the same thing; this is an entirely a new jurisdiction altogether and Ms. Drakes you can correct me where I am wrong but the Court in the Computer Misuse Act was the Marshal's Court correct?

Mr. CHAIRMAN: Sorry I did not hear the question?

Senator G. P. B. NICHOLLS: The Court which had jurisdiction over the Computer Misuse Act was the magistrate's court for the crimes?

Mr. CHAIRMAN: Yes. I think it was.

Senator G. P. B. NICHOLLS: Yes, so that if we use the strict Hinds analysis and not the simplistic Hinds analysis, this is not taking away jurisdiction of the High Court and giving it to a bench of magistrates.

Mr. CHAIRMAN: Remember the penalty was a lot less. $10,000 dollars if I remember.

Senator G. P. B. NICHOLLS: This is still not taking away the jurisdiction of the High Court and giving it to magistrates. We either need to deal with the Barbados Bar Association's analysis but I do not agree that you can have a scheme within a legislation where all of the offences carry or tried indictably but then we pick out two (2) and say that they can be charged either way.

Mr. CHAIRMAN: The alternative is to just put this on indictment like all the rest.

Senator G. P. B. NICHOLLS: It lacks internal consistency. If this is a policy reason, I do not accept that you will get tried faster in the magistrate's court. That cannot be a policy reason and to satisfy the Barbados BAR Association we will reduce the fine? What happens to the victim?

Mr. CHAIRMAN: Okay, so your view is to just put them like all the others on indictment. That is correct?

Senator G. P. B. NICHOLLS: Not just because the Barbados Bar Association says, I could be a lone dissenter here but not because the Barbados Bar Association says that is unconstitutional. Parliament is powerless now to create offences and punishments?

Mr. CHAIRMAN: Alright. We put 19 and 20 on indictment like all the others but to leave the penalties.

Ms. RHEA DRAKES: Noted, Mr. Chair.

Mr. CHAIRMAN: Okay so we were at 23 and we said Ms. Drakes, we would look at that Proceeds and Instrumentalities Act for consistency on this issue? Section 22(d); 23(2)(d), sorry. Anything on assisting a police officer, Clause 24? Clause 25, Record of seized data to be provided to owner. If none on those, Clause 26. The Production of data or criminal proceedings.

If nothing, Expedited preservation and partial disclosure of traffic data, Clause 27.

Ms. RHEA DRAKES: Sorry, Mr. Chairman, if we can go back to Clause 23(2)(a), I have a note to include the words *"or contains evidence"*. It should read, *"A warrant issued under this Section may authorise a police officer to seize or similarly secure any computer system, data, programme, information, document or thing, if you reasonably believe that it is evidence or contains evidence that an offense has been or is about to be committed."*

Mr. CHAIRMAN: *"... if you reasonably believe that it is evidence or contains evidence ..."*

Ms. RHEA DRAKES: Yes. That is my note from a previous meeting.

Mr. CHAIRMAN: Okay. Clause 28, The preservation of data for criminal proceedings.

Clause 29, Order for payment of compensation.

Any issues with that as presently drafted?

Clause 30, The legal capacity to make regulations.

The consequential amendments and obviously numbers 32 and 33, speak naturally "Repeal of the Computer Misuse Act" and coming into operation on a date fixed by proclamation.

The Mutual Assistance in Criminal Matters (Amendment) Bill follows from this. An amendment to the present Act. Is there anything any Member has seen in this Act which obviously follows from the Cybercrime Bill that you would wish to propose that we look at for amendment purposes?

This gives the framework for the prosecution of individuals outside of Barbados. Ms. Drakes, is there any issue with this Act?

Ms. RHEA DRAKES: Mr. Chairman, none that I can recall were raised in any of the previous meetings.

Mr. CHAIRMAN: What I am seeing is that, in a lot of cases, the Clauses in this Act speak towards Commonwealth countries. Why is it limited to Commonwealth countries in this Act considering, obviously, Budapest is much wider than Commonwealth countries?

Ms. RHEA DRAKES: I am just trying to open the document. Give me one (1) second.

Mr. CHAIRMAN: No problem.

Ms. RHEA DRAKES: Thank you.

Senator G. P. B. NICHOLLS: Mr. Chairman, are you asking why the Mutual Assistance in Criminal Matters (Amendment) Bill is limited there?

Mr. CHAIRMAN: Yes. I am seeing clauses saying Commonwealth countries as opposed to countries. Let us say that Barbados has mutual assistance agreements with,. so I just want to invite …

Senator G. P. B. NICHOLLS: Remember this is an Act that is amending an existing piece of legislation, so the policy consideration here is, in other words, the Mutual Assistance in Criminal Matters (Amendment) Act would have come up within a certain framework dealing with Commonwealth countries first; long before this Budapest Convention has become an issue.

If we adopt this legislation, we then become eligible to sign the Budapest Convention and then the Convention becomes Barbados' law or I should say instead of we becoming signatories to the Convention and be accede to the Convention on the basis that we have a domestic law in place

that is Convention compliant; so that I do not see the need for us, as a Committee, to be tinkering with the Mutual Assistance in Criminal Matters (Amendment) Act to expand the language accommodative of country in which we are in mutual accord. In that specific context, I do not think we need to …

Mr. CHAIRMAN: I understand you, that the parent does not speak to Commonwealth countries alone and this is just an amendment to that Act.

Senator G. P. B. NICHOLLS: Yes, to allow us to give similar terms of mutual assistance that we will give under this Act, to the members of the countries that we will sign onto with the Budapest Convention. That is the purpose of the amendment, but not to, as a substantive consideration as to expanding the scope of the Mutual Assistance in Criminal Matters (Amendment) Act to countries outside of the Commonwealth. I think that would be outside the scope of our remit as a committee.

Ms. RHEA DRAKES: Senator Nicholls has answered some of what I was going to say. The amendments to the Mutual Assistance in Criminal Matters Act related mainly to the powers that are currently found in the Computer Misuse Act in Part III, The Investigation and Enforcement in terms of the assistance in expediting preservation of computer data. In the Bill it is found, as I said, in Part III and Clauses 26 to 28 make provision in terms of preserving the computer data that would include any necessary orders so that you can save it; preserve it, you can go back and get an extension for the preservation of the data.

Also in 20(b) which is also in the Bill, it relates to expediting disclosure of the preserved traffic data. For example, who is the service provider and sharing that information with the central authority. It has not gone too far from what currently exists. It was just to give it more teeth in terms of being able to access the information were the service provided, for example, is based overseas.

Mr. CHAIRMAN: Okay. Thank you for that explanation. Atre there any other considerations of the Bills that any Member would wish to raise? The Clerk of Parliament has indicated that he can get to us an edited transcript of this meeting today by when, Mr. Eastmond?

Mr. CLERK: Tomorrow, Sir.

Mr. CHAIRMAN: From that, let us see if we can get agreement on this. I want to repeat: Let me do a draft outline of the proposed amendments that we have agreed on or that there have been no objections to; before this Committee and submit to Members before we next meet for consideration for us to come and discuss at that next meeting which would hopefully be the last meeting; our last meeting before the Report starts being crafted. When can be our next meeting?

Senator G. P. B. NICHOLLS: Mr. Chairman, I am not sure what is the Agenda for the next meeting. Are we looking at a draft report? What is the Agenda for the next meeting?

Mr. CHAIRMAN: Like I said, I would do proposed amendments as gleaned from our discussion.

Senator G. P. B. NICHOLLS: I am not understanding. I thought that was what we just did. No?

Mr. CHAIRMAN: Okay. Mr. Eastmond, your guidance here. Do you have enough that your staff can glean proposed amendments.

Mr. CLERK: Sir, I am waiting on the AI of today's meeting.

Mr. CHAIRMAN: Explain.

Mr. CLERK: The edited version of the transcript, which is what we had agreed on and then we do a draft of the proposed amendments.

Mr. CHAIRMAN: You tell me. Certainly I am going to need some assistance, though, from your staff with that. This is not the first time there has been a Select Committee. How was it done, for example, with the Child Justice and Child Protection Bills? Okay. Honourable Member, Leader, before you go, when is the date you can be available. Thursday afternoon? Remember we have to give a Report on the 14 June, 2024. This Thursday. How was it done with the Committee on the Child Justice/Child Protection Bills? Who would have formulated the amendments that came out of the Committee meeting?

Ms. DEPUTY CLERK: Mr. Chairman, thanks for the question. I would have compiled

all of the amendments that were discussed during the nine (9) meetings that we had and sent them off to the two (2) parent Ministries: The Ministry of Home Affairs and the Ministry of People Empowerment with the input of the Chief Parliamentary Counsel (CPC) as well.

Mr. CHAIRMAN: That was before the Report was written?

Ms. DEPUTY CLERK: Yes, please.

Mr. CHAIRMAN: Okay, that is what I want guidance on.

Ms. DEPUTY CLERK: After that, the Committee will come back and go through and approve.

Mr. CHAIRMAN: If the Senate has only given us to the 14 June, 2024, how soon then did the parent Ministries take to get back?

Ms. DEPUTY CLERK: As Mr. Eastmond just indicated, we need the transcripts.

Mr. CHAIRMAN: Which he is saying we can get tomorrow, and then you formulate.

Ms. DEPUTY CLERK: Then the AI would give us some leverage.

Mr. CHAIRMAN: In this case, the parent Ministry, we would have to indicate to them the constraints.

Ms. DEPUTY CLERK: As it relates to the policy decisions. Right.

Mr. CHAIRMAN: Then we wait until they respond.

Ms. DEPUTY CLERK: Yes, and then you would have one final meeting with the Committee to agree on those recommendations.

Mr. CHAIRMAN: Okay.

Senator G. P. B. NICHOLLS: Mr. Chairman, I think we are not being clear on the steps. I understand at this stage that the Clerks will decipher or discern what are the recommendations coming from the deliberations of the public consultations and the persons who appear before us and our own internal analysis of all of those recommendations and dealing with the matter for the last amount of weeks. They will send a Report to the parent Ministry which will comment on the Report. If there are recommendations of a policy nature, where things need to be changed; coming out of the Select Committee's deliberations, the parent Ministry will comment on those and then they will come back to us as a final Report. Is that my understanding? Is that process correct?

Ms. DEPUTY CLERK: Yes, please.

Senator G. P. B. NICHOLLS: Mr. Chairman, that was what I was saying. We are getting a little backwards. I do not think we need to be setting a date for our meeting because we would not have anything to do….

Mr. CHAIRMAN: Right, so based on that we will not set a date on our meeting, no. So who is going to take responsibility then? You again, Ms. Gibbons?

Ms. THE DEPUTY CLERK: That is okay. Yes, I will do it.

Mr. CHAIRMAN: So we do not set a date for our meeting.

Senator G. P. B. NICHOLLS: Mr. Chairman, rest assured again, to the extent that we have a Computer Misuse Act in place right now, it is still the law of Barbados; it covers a number of things. If the Senate has to give an extension so that the process can be completed, I understand from the Minister and I checked with her after we met on the last occasion, that it is not that we need to get this done before World Cup because there is going to be any particular threat.

There are always threats to your cybersecurity, that is the truth. The legislation does not evaporate those threats but it puts you in a position to be able to communicate with who you need to communicate with in order to mitigate or to deal with them effectively. I am just saying that we should not be under the impression that we are under a rush to complete this process because the Senate's allowance of time is unmerciful. Okay?

ADJOURNMENT

Mr. CHAIRMAN: Agreed. Okay, so is there a Motion to adjourn.

On the Motion of Mr. P.R. PHILLIPS, seconded by Senator the Honourable L.E. NURSE, the question that the meeting be

adjourned sine die was agreed to, and THE CHAIRMAN adjourned the meeting accordingly.

Mr. CHAIRMAN: We adjourn then *sine die* pending the processes here now. Is there agreement that you will try to get the unedited transcript of today's meeting to us tomorrow? Thanks, everyone. Thank you, Ms. Drakes, for being present.

Ms. RHEA DRAKES: You are welcome. Thank you for having me.

Mr. CHAIRMAN: Senator Nicholls, thanks for joining even though you are not in Barbados.

Senator G. P. B. NICHOLLS: Thank you, Mr. Chairman and may I also record my appreciation for the Clerks and everyone who facilitated. Thanks, Ms. Drakes, for coming today and for giving her time with us. Thank you.

Mr. CHAIRMAN: As I understand it, we have snacks available which you will not be able to participate in, Senator Nicholls.

Senator G. P. B. NICHOLLS: Yes, I am in Guyana at the mercy of the post-Independence celebrations. Good afternoon, colleagues.

Mr. CHAIRMAN: Good afternoon. Goodbye.

7th MEETING
JOINT SELECT COMMITTEE (STANDING)
ON
GOVERNANCE AND POLICY MATTERS
ON THE
CYBERCRIME BILL, 2024
AND THE
MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024

Thursday July 4th, 2024

PRESENT:

Mr. Edmund G. HINKSON, S.C., MP, LL.B. (Hons.), L.E.C., LL.M. **(Chairman)**
Dr. Romel O. SPRINGER, J.P., MP., PH.D., (Deputy Chairman)
Mr. Peter R. PHILLIPS, MP
Mr. Ralph A. THORNE, K.C., LL.B., L.E.C., Dip. Theology
Senator The Hon. Lindell E. NURSE, F.C.A, F.C.C.A., R.C.S. (ENT)
Senator Ryan O. WALTERS, M.B.A.

ALSO IN ATTENDANCE:
Mr. Pedro EASTMOND, (Clerk of Parliament)
Ms. BEVERLEY GIBBONS, (Deputy Clerk of Parliament)
Miss Suzanne HAMBLIN, (Journal Department of Parliament)

ABSENT:
Senator Gregory P. B. NICHOLLS, B.Sc. (Hons.), LL.B. (Hons.), LL.M., MCIArb.
Ms. Rhea DRAKES, (Office of the Chief Parliamentary Counsel)

Call to Order
The Chairman called the meeting to order at 2:45 p.m.

Mr. CHAIRMAN: Good afternoon, Honourable Members and staff. Thanks for coming; we have had a lot to contend with this week. Of course, we know we were to meet on Monday but that would have been virtually impossible and we are meeting this afternoon, so thanks for coming.

Everyone would have seen the Agenda. I am calling the meeting to order. Welcome. First, we have four (4) sets of Minutes to look at and Minutes of our third meeting which was held on 06 May, 2024. We take them as read and we assume everyone has read them. I went through them yesterday and I am proposing some, in all cases, quite minor amendments to each of them.

We will do the third meeting first. I just wanted on page two (2), the second last name, the capital "*C*" for the word *"Cybercrime*" for consistency purposes.

Then on page three (3), the first, full paragraph, the third last line put a full stop after the words *"Budapest Convention"* and that is on line 11 of page three (3) and start the next sentence with *"Even". "Even so this clause itself uses outdated language …"*

In the line after that, *"He stated that if something is temporary …".* I think that is a typographical error there. Switch with the word *"is*" to make it, *"is temporary …".*

Dr. R. O. SPRINGER: Is there supposed to be another word before "*and"* unless the "*and"* was the error.

Mr. CHAIRMAN: I interpreted it to mean the "and" was a typographical error. He said that, *"… if something is temporary and does not cause harm …*"

Dr. R. O. SPRINGER: So "*and*" is to be replaced by "is".

Mr. CHAIRMAN: "*And*" is to be replaced by "*is*" and then on page four (4), the 4th line, *"He opined that in relation to this section …",* put in your word "*to*". At Page four (4), line four (4) it should state, *"He opined that in relation to this*

section …".

Then page five (5), line six (6), *"… those actions which though well intended could cause harm"*, so the words are "*actions which".* Those are the words to put into the sentence, *"As regards to activist, it was the judiciary's duty to determine the difference between malicious intent and those actions which, though well intended, could cause harm."*

Then on the next page, page six (6), the third paragraph, the 4th line. Let me read the whole sentence from line three (3): *"Mr. Williams responded that he was not aware that any specific area had more attention than others but that when the Computer Misuse Act was drafted, there was limited social media, compared to the present time."* I think what the Minutes said, *"there was no social media"* and Mr. Williams clearly did not say so; so I am proposing to put in the words, "*there was limited social media compared to the present time".*

Then on page seven (7), the third paragraph just before, *"Mr Anthony Greene, General Manager, STARCOM Network the words, "Mr Caswel Franklin"*. I think *"Caswell"* is misspelt there. *"Caswell"* if I know it has two L's.

Then the first paragraph under, *"Mr. Anthony Greene …"* on that page, page seven (7), **line two (2),** "*the content of the Bill to address the perceptions that have arisen from the debate"*. *"Mr. Greene began his presentation by noting that due to the timelines of the Committee, he opted for an oral presentation and that he was not fully prepared to address specifically the content of the Bill, to address the perceptions that have arisen from the debate."*

Then in the next sentence, replace the word "*designating*" with the word "designated". "… *to consider how the country communicates, not just facilitating designated information but also empowering citizens to actively engage in discussions."*

Then on page eight (8), in the first line. *"He also expressed concern that journalists or media personnel …"* so take out one of the "*that*s", add on an "s" on *journalist; "or media personnel should be allowed to receive and report on information."* Take out the word *"received"* and put in the word "*receive".*

Then on page eight (8), the last paragraph under the heading of *"Dr. Ferdinand Nicholls*", the word "*pulpit*" in the third last line. The "*t*" is omitted, I believe, from the word *"pulpit".* In the word "*pulpit*", add on the "*t*" and then add a comma afterwards.

In the last sentence of that paragraph, *"He opined that the Bill uses language that is "open" to being deemed as vague, …"*

Those, in my opinion, were the amendments that are required. Did anyone see any others?

Mr. CLERK: Mr. Chairman, I want to take you back to Mr. Williams.

Mr. CHAIRMAN: Okay.

Mr. CLERK: I would suggest that rather than, as you would have suggested, the note have *"there was no social media"* and you said that *"there was limited social media"*, but Mr. Williams did say so.

Mr. CHAIRMAN: He said, "*no social media?"*

Mr. CLERK: Yes, but, I think, what we can put in, because he went, *"not in the way that we have it today",* so I would just make a slight adjustment, stating no social media especially in its current format or something to that effect.

Mr. CHAIRMAN: Did he say that there was no social media?

Mr. CLERK: Actually, this is what he said: *"I think given the fact that I would appreciate that when we had the Computer Misuse Act, there was no social media. When we had the Computer Misuse Act, there was no such thing as social media, especially in its current form" or something like that, especially as we know it today.* Something to that effect he was suggesting.

Mr. CHAIRMAN: He said especially in its current form?

Mr. CLERK: Yes.

Mr. CHAIRMAN: All right, so that when the Computer Misuse Act was drafted there was no social media as it relates to social media in its current form?

Mr. CLERK: No social media *as we know it today.*

Mr. CHAIRMAN: Alright, that is good. There was no social media as it currently exists. Okay, so do you wish to do Matters Arising from these Minutes now or do all the amendments first and then Matters Arising?

Asides.

Mr. CHAIRMAN: Okay, any Matters Arising from these particular Minutes of the third meeting? If none, let us go on to the fourth

meeting then. Okay, so Motion to confirm the Minutes as amended of the third meeting? To move that the Minutes as amended are confirmed.

The Motion that the Minutes of the third meeting of Monday, 06 May, 2024, as amended, be confirmed was put by Dr. R. O. SPRINGER and seconded by Mr. P. R. PHILLIPS.

Mr. CHAIRMAN: Are there any Matters Arising from these Minutes, which anyone wishes to discuss? Okay, we have the Minutes of the fourth meeting of 13 May, 2024, as presented and again, I propose the following amendments to these Minutes: Page three (3), at the third line which starts as follows, "*Mr. Chairman pointed out that this recommendation",* we must put in the word "*final"* so that it reads *"Mr. Chairman pointed out that this final recommendation would just add to more bureaucracy".* Are you seeing it, Members? Then, there is the last line on Page four (4), which is under Mr. Timon Howard.

Asides.

Mr. CHAIRMAN: It is the second sentence of his presentation, and reads: *"... freedom of expression which he believes was a natural right was being violated under cyberbullying".* Then, in the next sentence he stated "the defences as provided pursuant to Clause 19(5) *were clear*"; the word *"were*" is inserted.

Then, next on my Page six (6), where we started in terms of questioning Minister Caddle. Members of the Committee questioned Honourable Minister Caddle, they were to put in the word "*Members*". Are you following?

Mr. CLERK: Yes.

Mr. CHAIRMAN: Then, the next paragraph, in other words, the paragraph before item five (5) – Any Other Business. Again, you can tell me from Hansard but I wanted to put in "*alleged offences*". In other words, "Honourable Minister Caddle was asked whether the Bill would capture persons within Canada, USA and England, who would have committed *alleged offences*.

Again, for clarity purposes, under Any Other Business, third line, which is at the bottom of my page six (6). "*It was agreed that Senator Gregory P. B. Nicholls would request an extension*" and I put in the words, *"from the Senate".* This is just for the sake of completeness; an extension from the Senate of time for the Committee to complete the report.

Were there any other amendments Members would wish to suggest? If not, can I have a Motion for these Minutes to be confirmed as amended?

Dr. R. O. SPRINGER: Mr. Chairman, I beg to move that the aforementioned Minutes be confirmed as amended.

Mr. P. R. PHILLIPS: I beg to second.

The question was put and resolved in the affirmative without division.

Mr. CHAIRMAN: Are there any Matters Arising from these Minutes of the fourth meeting? If there are no matters arising, let us look at the Minutes of the fifth meeting, held on Thursday, May 23, **2024**. Taken as read. I wish to propose the following amendments.

This is my page three (3). Barbados Consumer Empowerment Network under that clause, the second line. "*He believed that this observation did not have merit as regards this particular Bill as opposed to other possible legislation".*

Then, on my page five (5), when we were discussing Clause 19 (4), in other words, just before item five (5) – Any Other Business, just the 'B' 'A' 'R' because earlier on we had said Barbados Bar Association is BAR. Therefore, in the interest of the BAR's comments and submissions.

Then the last sentence of that particular paragraph, just before item five (5) – Any Other Business, Niel Harper's submission, to be discussed in the presence of the draftsperson.

Then, just before adjournment, which is at the top of my page six (6), Ms. Rhea Drakes would be available. The Committee agreed that the next meeting would be held on Monday, May 27, **2024**, when the draftsperson from CPC, Ms. Rhea Drakes, would be available. Then, just to put in the word "adjourned" under adjournment. On the second line, Senator the Hon. L. E. NURSE adjourned.

Asides.

Mr. P. R. PHILLIPS: Mr. Chairman.

Mr. CHAIRMAN: Yes, Honourable Member.

Mr. P. R. PHILLIPS: There is a slight

typo. My surname carries two *L*'s.

Mr. CHAIRMAN: Okay. It is okay at the top but not at the bottom. Motion for confirmation of these Minutes of the fifth meeting as amended.

Mr. P. R. PHILLIPS: Mr. Chairman, I beg to move that these Minutes be confirmed as amended.

Dr. R. O. SPRINGER: I beg to second.

The question was put and resolved in the affirmative without division.

Mr. CHAIRMAN: Are there any Matters Arising from these Minutes? If there are no Matters Arising, can we move onto the final one (1); the Minutes of the sixth meeting of the Committee, held on Monday, 27 May, **2024**. I take the Minutes as read. I wish to propose a few amendments.

On Page four (4), under item three (3) – Consideration of the Bills, second paragraph, the last line. She noted, and this is Ms. Drakes we are talking about, she noted that there can be references *or* portions of legislation. I think it might be a typographical error. The word "portions" between *or* and *of* legislation.

Then the next paragraph, which is my last paragraph on page four (4), the paragraph starting the Clerk opined. The report goes back to the House of which it was originated or it should be from I would think. *"The report goes back to the House", "from"* instead of *"of which it was originated"* and that House then debates and adopts with "*t*s" or rejects with "*ts*". Any suggestions or amendments proposed by the Committee?

Mr. CLERK: Mr. Chairman, I would say that there is no need to put the "*was*" there if the report goes back to the House from which it originated.

Mr. CHAIRMAN: From which it originated. Yes. So, to omit the word "was" as well. Again, at the end under the adjournment right at the end, Mr. Phillips' name is missing the second "l". So, there being no further business, *"On motion by Mr. P. R. PHILLIPS seconded by the Senator, The Hon. L. E. NURSE, the meeting was adjourned sine die".*

I wanted to just be sure since we picked up those two misspellings of the Honourable Phillips' name, to make sure in the first two (2) that…. That one (1), it was Senator Gregory Nicholls and Dr. Romel Springer for the first. Let us see for the third. In the third, Phillips was spelt correctly. In the Minutes of the third meeting on the adjournment, Phillips is correctly spelt with two (2) "l's".

So, it is the last two (2) Minutes that we looked at to correct the spelling of Phillips by putting in the second "l" in each of them. So, I invite the moving of a Motion for confirmation of Minutes of 06 May, 2024, meeting.

On the motion of Mr. P. R. PHILLIPS seconded by Dr. R. O. SPRINGER, the Minutes for 06 May, 2024, as amended, were confirmed.

Mr. CHAIRMAN: Motion so moved. Minutes confirmed as amended. Any matters arising under the Minutes of meeting on 06 May, **2024**? Okay. If none, we move on to Item No. four (4); Consideration of the Proposed Amended Bill.

I will give Members an opportunity to pull up the amended Bill which would have been sent to us by Parliament. Do you have the date when you sent it? 02 July, **2024**? Not July. You circulated that a long time before that. You sent it again on Tuesday? This one (1) has the highlights for the…? Same one? Okay.

Mr. CLERK: Dated, 18 June, **2024**.

Mr. CHAIRMAN: Right. Okay. It is here. That is correct. It was sent in the package with the Minutes again on Tuesday. This is my package here? Oh. I did not even realise. Okay. Okay, it is in the package too. Right.

So, we are going to go through this again. I just want to mention too because obviously, we are considering with this that I would have requested comments from the Office of the Director of Public Prosecutions (DPP) to the comments made by the Barbados Bar Association (BAR). And those were circulated. I just want to be sure everybody saw them, the comments of the Director of Public Prosecutions' Office, in relation to comments made in the submissions from the Bar Association.

Clearly, the DPP's response, we would wish to have included in the report too as a submission. No objections

to that from anyone? No? Okay. Let us look at the proposed amendments as submitted by the Office of the Chief Parliamentary Counsel (CPC) on our instructions based on what we discussed at our last meeting. So, the first amendment to the

Bill proposed is the definition of cyberbullying where we asked for a definition of cyberbullying to be included in the Bill.

We could also have present in the notes. Right? That is the DPP's Office business as well. Notes. Okay. So, put in a definition of cyberbullying. Cyberbullying means the behaviour or conduct referred to at Section 20. I do not think anyone would have any issue with that. Section 20 is where cyberbullying is spoken about.

Asides.

Mr. CHAIRMAN: We will come down to that. We are taking it step by step. Senators, are you comfortable with that definition? As I said, that is how drafters in Barbados draft that definition. So, in my opinion, there is no problem with that. We wanted a definition of *"without authority"*.

The definition given is, *"without right, consent, permission, authorisation or in excess of authorisation"*.

Dr. R. O. SPRINGER: I know we discussed that here but you see, in certain organisations, anybody could…. Sorry. I believe that this is a bit too vague or too broad because anyone can give authorisation. That authorisation should come from a person who has the authority to grant such, because very often you have a case where a person may call in, and this is not cyber related. This happens in the real world but it is an example of how it can work in a cyberspace scenario where a person calls into an office and speaks to a clerk or someone at that level; that person in turn grants them permission to do something when in actual fact that person does not have the authority to grant permission but the argument could be made when the situation comes to a head that permission was granted by the office by a person in the office; almost similar to what we get often when people go to government offices and the clerks and sometimes the guards tell them things and they take that as gospel and they go with it.

Mr. CLERK: So what happens if the same person gives them permission?

Dr. R. O. SPRINGER: What happens if…?

Mr. CLERK: If the same person gives them permission?

Dr. R. O. SPRINGER: The same person who is not authorised to do it?

Mr. CLERK: Yes, gives them permission. You are saying that you need to get authorisation but if the same person says that you have permission to do it.

Dr. R. O. SPRINGER: Right, but I believe that you should make it clear that the person who grants the permission has the authority to grant the permission and is not just a person who works within the organisation, because that can happen. People will come, like you are the authority here. along with Ms. Gibbons. You are both authorities, yet if someone comes here and speaks to the security downstairs and he is given authority to tour the building or to come in here or what have you…

Mr. CHAIRMAN: And that is why you have "*in excess of authorisation*" right?

Dr. R. O. SPRINGER: This has *"if the person acts in excess of the authorisation that they were given"* but they could have been given authorisation to do anything but the person who gives the authorisation will be acting ***ultra vires*** because they do not have the right to do it. So we must make it clear that it must come from a person with the authority to grant that permission or that authorisation; if we can make that clear. You understand my point?

Mr. CLERK: It is taken that when you have *without authority* that the person who gives that authority has to be someone who…

Dr. R. O. SPRINGER: I do not think that we should, and I know the spirit of it, but the wording of it does not suggest that.

Mr. CHAIRMAN: You could only go by…

Dr. R. O. SPRINGER: People give consent to things that they really do not have the right to give that consent**.** We must have an argument if it comes to that.

Mr. CLERK: Then the person did not really get consent.

Mr. CHAIRMAN: If someone who does not have the authority or the right to give consent; it is not consent.

Dr. R. O. SPRINGER: It will just take an additional few lines to make it clear that the person must be an authorised person.

Mr. CHAIRMAN: I do not know, and again you see this is taken from another piece of legislation because I think I saw this …

Dr. R. O. SPRINGER: The exact words?

Mr. CHAIRMAN: Yes. I saw this in the USVI (Virgin Islands) version because remember it was me who said to put in *"in excess of*

authorisation" and this is how it is phrased in that.

Mr. CLERK: My view is that if you see that, it means that if someone gives authorisation that is not authorised to do so; you did not get any (consent) at all.

Mr. CHAIRMAN: I think it could be made clearer though.

Dr. R. O. SPRINGER: You see where the challenge can come? You think we could make it clearer

Mr. CHAIRMAN: I do not think so…

Dr. R. O. SPRINGER: Do we not deal with specifics? We do not deal with specifics in law?

Mr. CLERK: When we say without authority, it means without authority**.**

Mr. CHAIRMAN: No.

Dr. R. O. SPRINGER: We are in a territory where authority is granted by someone within the organisation, to use the computer to access certain files. You got the authority of someone at a lower level and you go ahead and you commit whatever crime. The argument then comes later on that you did not get authority from the Management Information Technology (MIT) Manager or the Management Information Systems (MIS) Manager, who was the rightful person that should have given the authority. Maybe the authority was given to you by one of the other technicians and you would not necessarily know that and that the person was not authorised to give you the okay.

Mr. CLERK: If you use that example in an office for instance; where computers, well I do not think anyone needs any authority because you have a computer and so do I, and I go and use it. Beverley has a computer and …

Dr. R. O. SPRINGER: Everything is all well and good until something goes awry. It is all well and good that anyone can give the okay to log onto this system; it is when information goes missing or when something is corrupted or something is shared that should not be shared, is when you get down to who gave you the right to access these files and then this here, a person may say '*well I was given the right by Senator Walters'*. He was my immediate supervisor and he told me that I could access the files, and someone would be arguing that he does not have the right or clearance to give you that access.

Whose fault is that now? Is that my fault or Senator Walters' fault? Who did it with all good intentions or should it be clear that the argument cannot be used because it is written specifically in the legislation that the person who grants the authority must be a person who has the authority and that is not there but**...**

Mr. CLERK: Mr. Chairman, I do not know if you need to add that. I feel like the authority …

Mr. CHAIRMAN: I do not know. You might be able to use that in mitigation of the offence but yes, I do not think so.

Dr. R. O. SPRINGER: I just am trying to give it a layman's scenario.

Mr. CHAIRMAN: You might be able to use that, as I said. in mitigation that you thought this person had the authority, where they did not but I do not know that you could water this down any more.

Dr. R. O. SPRINGER: Authorised personnel or something like that. There is some word or terminology that captures what I mean by a person with proper clearance and the proper authority to grant permission. It might just be an extra two (2) words or three (3) but I feel gentlemen, as lawyers, believe this captures exactly what…

Mr. CHAIRMAN: I do not think so and like I said I have seen it like that. I think in the US Virgin Islands one that was sent to us; so I do not know. You have to be careful with watering down this Bill too much.

Dr. R. O. SPRINGER: I was thinking it was tightening it up.

Mr. CHAIRMAN: Look at five (5) for instance, Clause five (5). That any modification referred to in Subsection four (4) is without authority, *"If the person who causes the modifications knows he is not entitled to determine whether the modification should be made"*. You see, the person again, it still boils down to *mens rea*. You know you are not entitled to determine it, so you know you are acting without authority.

Dr. R. O. SPRINGER: I also know I was granted some level of authority by someone. If I could share. This is off the record.

Asides.

(Remarks made by Dr. R. O. SPRINGER were inaudible for more than four (4) minutes as he turned off the microphone)

Mr. CHAIRMAN: In terms now of the public interest defences that were put in between

Clauses four (4) – 11, with the exclusion of Clauses nine (9) and 10. In other words, Clauses four (4), five (5), six (6), seven (7), eight (8) and 11.

Senator Gregory Nicholls, of course, who is unable to make it today and he gave an excuse, but he had said, and I am willing to agree with him now, withdrawing that public interest defence.

Dr. R. O. SPRINGER: I am in support of that.

Mr. CLERK: So are we taking it out?

Mr. CHAIRMAN: Yes.

Asides.

Mr. CHAIRMAN: Right. In other words, going back to the original but you know other Members who are willing to …

Dr. R. O. SPRINGER: I think this is a good idea. I felt that public interest defence would almost open the doors to that discussion about ethical hacking and such like -- that I never supported. Also, anyone can make the argument that they are doing something in the public's interest, even if it is unethical; it is immoral and it is wrong. If you think you are doing it for the greater good and for all humanity, then that that could be your argument and your excuse. I do not think it should ever exist.

Mr. CLERK: Senator Nicholls has agreed to that?

Mr. CHAIRMAN: Yes, he has.

Dr. R. O. SPRINGER: The Minister has also …

Mr. CHAIRMAN: If it is going to be problematic, they are bringing in the legislation for other areas that will also encompass that kind of defence. From speaking with Sir David Simmons as well; I spoke with him on it and he said that they did not recommend that when they spoke with the experts from the European Commission, for instance and that is why they did not put it in in the original Bill, in the Bill as presently drafted.

Mr. CLERK: So are we taking that out in Clause four (4)?

Mr. CHAIRMAN: In all of them.

Mr. CLERK: Right.

Mr. CHAIRMAN: The ones they were in are Clauses four (4), five (5), six (6), seven (7), eight (8) and 11.

Mr. CLERK: This was just an additional subsection so once you take that out, the Bill goes. I think that came at the end of each Clause.

Mr. CHAIRMAN: Right, at the end of each Clause so that additional subsection is to come out but at 13(2), where we substituted the word *"or*" instead of the word "*and*" that is good. To move to Section 19.

Mr. CLERK: Are you only going to where the amendments are?

Mr. CHAIRMAN: Yes. We went through everything else already. We are only dealing with the amendments now. At least that is my proposal, to look at the amendments as drafted.

So Section 19, the issue here with Section 19 is how it is going to be tried and I would appreciate some discussion on this. The Bill as presently drafted has that Section 19 and 20 would be tried summarily, in other words, by a magistrate. Those are the only two (2) offences under the Bill that the Bill, as presently drafted, which propose that they were be tried by a magistrate and not by a judge.

We had asked that that be changed to be tried by a judge by indictment. The Director of Public Prosecutions (DPP) in response to the Barbados Bar Association which I mentioned at the start of this particular Item on the Agenda, had said that putting it by indictment they preferred not to; that judges already have a lot of work and are overburdened. I am proposing, as is done in Guyana; in Jamaica; in Belize and in the United States (US) Virgin Islands, that an option be given to the accused to be tried summarily or by indictment.

The last piece of legislation, which was before what we are doing now and after the Resolution on Population Study; the piece of legislation that was passed in the Honourable Lower House had given an accused the option to be tried by jury or by judge alone**.** Similarly, I am proposing that we put Clauses 19 and 20 as hybrid offences, where the accused be given the choice whether to be tried summarily or by indictment.

That, in my opinion, resolves whatever issue the BAR Association may have had or had that to try offences before those two (2) Clauses before a magistrate is unconstitutional on the basis of ***Hinds vs The Crown***; a Jamaican case that went to the Privy Council. Both Senator Nicholls and I, as attorneys-at-law, have said that we do not agree with the Bar Association's submission but out of an abundance of caution, if a court were to agree with the BAR Association's position and disagree

with Senator Nicholls and myself, that it is a breach of the Constitution; I am proposing that the accused be given a choice either to be tried summarily or by indictment. That is done in all of the other Caribbean Community (CARICOM) countries plus the United States Virgin Islands which have a similar Clause 19, the Malicious Communication clause.

I am also proposing that as is in each of those, that the sentencing options available to the judicial officer differ but in each of those jurisdictions, the fine and the imprisonment is the maximum, I should say. It is less if you opt to be tried before a magistrate than if you opt to be tried before a judge. I am proposing that on summary trial …. Remember it is always a maximum and you cannot bind the presiding officer's discretion in this case; so that if it is tried summarily, that the maximum fine should remain at $70 000; the maximum term of imprisonment should remain at seven (7) years but if you opt to go before the judge to be tried on indictment, that the maximum fine should be $100 000 and the maximum term of imprisonment should be ten (10) years, or both. That is $100 000 before a judge or imprisonment for ten (10) years, or both.

Remember these are just maximums beyond which a presiding officer cannot go. The presiding can say, *"You are convicted but I am just reprimanding and discharging you" or fining you $1 000"*. Under our Separation of Powers concept, Parliament cannot intervene in that.

Asides.

Mr. CLERK: So those are Clauses 19(1), (2) and (3)?

Mr. CHAIRMAN: Wherever they say the penalties, which would be 19(1), (2) and (3), yes, and 20. Remember originally it was summarily. Yes, it would have to be re-drafted and, as I said, there are other laws like that in Barbados, where you have that option and, in terms of all the CARICOM and Caribbean countries that have this legislation, they have the Malicious Communication Provision.

Mr. CLERK: So the cyberbullying is the same thing as well?

Mr. CHAIRMAN: The same thing, Clause 20.

Mr. CLERK: Would that be either option?

Mr. CHAIRMAN: Either option. That is my proposal. What say Members? Again, this is after discussion with Sir David Simmons on this point. Like I said, with that option someone could not now, do what the Bar Association is concerned about; which is to say that it is unconstitutional to be tried before a magistrate because you would have the option to go before a judge.

Asides.

Mr. CHAIRMAN: It is an accused person's choice; that you have the option to go before the magistrate, where the possible fine or the possible imprisonment on conviction may be less or at least the maximum which a magistrate can sentence. A magistrate is less than what a judge can sentence you, but you cannot say that to go before the magistrate is unconstitutional because you have the option to go before the judge; your choice to be decided on, presumably, with your legal counsel.

It is just as we have just passed law; has it reached the Senate yet? It has passed the Senate too? Just as we have passed law that you have the choice to go before the judge alone or go before a tribunal of your peers, a jury.

Senator the Hon. L.E. NURSE: Recently, we passed an amendment where one can be tried by a judge and jury or a judge alone; would that affect any of the definitions which we have here? Would we need to be a little more expansive here in terms of the issues here?

Mr. CHAIRMAN: It would apply here too, that if you opt to go before the judge – in other words, to be tried by indictment – you would have that option under this legislation too; either for the judge alone to hear it or judge and jury. That under the Bill that was passed as the Criminal Procedure (Amendment) Act; you would have that option, if you opt to go by indictment.

Mr. CLERK: Even if you opt to go by indictment, when you get to the High Court you still have the option to either do judge and jury or judge alone.

Mr. CHAIRMAN: Welcome to the Opposition Leader, Honourable Ralph Thorne. We are at item four (4), where we are considering the proposed amendments that we asked for and on reflection, I am suggesting and I will repeat for your benefit, that clauses 19 and 20; the offences under malicious communication and cyberbullying respectively, that an accused person be given an alternative, the option rather, to either

be tried summarily or on indictment.

That is done in each and every one of the CARICOM jurisdictions that have this legislation. That option is given in the malicious communication clause. It is given in Guyana; Jamaica; Belize; US Virgin Islands and remember we were sent to the US Virgin Islands' one (1) about three (3) weeks ago. In each case, the accused has the option to be either tried summarily or by indictment. In my submission, it would also ***negatise*** the BAR Association's opinion. It is a submission which was noted as being prepared by Mr. Bryan Weekes, who incidentally as we all know, is now a Judge, that to be tried summarily is unconstitutional based on ***Hinds vs The Crown***. I think Senator Nicholls and I are on record last time saying that we do not agree with that submission, but still…it would do away with that because you would have the option to go on indictment if you wish.

As you know Honourable Leader of the Opposition, you spoke on the Bill two (2) or three (3) weeks ago. Parliament is now giving that option of judge alone or trial by jury. As is done in all of the countries where the option is given under malicious communication, and I think in one of them where they have the cyberbullying, that the maximum sentencing, discretion of the judicial officer differs.

I am proposing to leave it on summary conviction, the maximum fine of $70,000 or imprisonment for seven (7) years or both. Before the judge, the maximum fine of $100,000 or imprisonment of 10 years or both. We all of course know that there is judicial discretion, a judge might say I am only fining you $1,000 or whatever. For instance, in the US Virgin Islands, on this particular section, when you go by indictment the maximum fine is $250,000 or imprisonment of 15 years.

That is my proposal and Honourable Leader of the Opposition, when you came, I invited comments and Senator Nurse then asked in terms of the implications of this based on the Penal Criminal Procedure (Amendment) Bill. It was then explained to him that an accused who opts on indictment would also obviously have that option to be tried by judge alone or by jury as well.

Mr. R. A. THORNE: Help me with the procedure. When is this going back to the House?

Mr. CHAIRMAN: We went through the Minutes. You would see that we had to confirm four (4) Minutes, we did that as amended, making some procedures and I think in the last one (1), the Minutes of the sixth meeting, 27 May, **2024** at which you were present, it was said that the report that we do here goes back to the House from which it would have originated.

Mr. R. A. THORNE: My question is simple. Does this legislation go back to the House in the new form for debate?

Mr. CLERK: As you are aware, …

Mr. R. A. THORNE: I am not.

Mr. CLERK: Okay. The House has already passed this piece of legislation, the Lower House. In the normal course of things, if this had come to the Senate without this Committee and the Senate had proposed amendments; what you will discuss back in the House, would be to concur in the amendments made by the Senate.

Now, the Senate is obviously going to debate the report and the Bill. What goes back to the House is really just the amendments.

Asides.

Mr. CLERK: For concurrence and debate.

Asides.

Mr. CLERK: Well, it is a resolution to accept the amendments made by the Senate.

Mr. R. A. THORNE: If the Honourable Member for St. James North got up and said he wanted to say something about the amendments, would the Speaker allow him?

Mr. CLERK: Of course.

Mr. R. A. THORNE: Okay. That is fine.

Mr. CLERK: As I said, it is then for the House to say we agree or we do not agree with these amendments.

Mr. R. A. THORNE: Right, thank you very much.

Mr. CLERK: You are not debating the Bill.

Mr. R. A. THORNE: Yes, the Member for St. James North would just …….

Mr. CLERK: Whichever Member would just be restricted to the resolution seeking concurrence in the amendments. It is not a debate of the Bill all over again because the House has already done that.

Mr. R. A. THORNE: He has notice.

Mr. CHAIRMAN: What say Members on that proposal? Okay, if no objection, we make that amendment to the amendments.

The other issue is the word *"embarrassment".* Honourable Leader of the Opposition, we referred to the submission by the Office of the DPP, which I invited them to submit based on the BAR Association's comments and remember that was also circulated.

Mr. CLERK: Mr. Chairman, where are we right now?

Mr. CHAIRMAN: How do you mean?

Mr. CLERK: We have gone through Clause 19 but there was an amendment in Clause 19, about reputational injury.

Mr. CHAIRMAN: That is what I coming to now. We agree to these but the issue of the word *"embarrassment"*; the word *"embarrassment"* where it is in Clause 20. The word "*embarrassment"* is in Clause 20 but not in Clause 19.

The Office of the DPP; remember their argument was that it is okay to be in Clause 20 but in Clause 19, which I am not so sure makes legal sense. I note that the word *"embarrassment"* is in other legislations; certainly, in the Guyana one. I was proposing that it be put back into Clause 19. It is within the power of an accused or their counsel to argue that *"embarrassment"* is too vague and should not be in too broad in Clause 19. It is within the parameters of a court to sever the word *"embarrassment"* from Clause 19.

Dr. R. O. SPRINGER: We had brought that up. I know I had said at the time when we discussed it that we could perhaps use a stronger term like emotional trauma. But, then, it was made clear that emotional trauma or even

trauma is not necessarily seen in legislation. I saw *"emotional distress"* which basically means the same thing. I have seen….

Mr. CHAIRMAN: *"Emotional distress"* is in Clause 19.

Dr. R. O. SPRINGER: That can be used to refer to *"embarrassment"*. In fact, people are sued in North America, both Canada and the United States of America (USA). I suspect even in Mexico they are sued for emotional distress that is caused by cyberbullying and all such like.

I think that captures humiliation; it captures embarrassment for sure. If we use that, then maybe we would not have to use *"embarrass"* because even if I were to misuse a word and someone put it on social media or somewhere and made fun about it when they see me in public, I would be embarrassed but, I do not think that that is grounds to have someone prosecuted.

But, *"emotional distress"*, I think that has a much stronger connotation; it has a much stronger meaning.

Mr. CHAIRMAN: Your opinion, Honourable Dr. Springer, is that is to leave it as is in Clause 19, excluding *"embarrassment"* because it is covered by substantial emotional distress.

Dr. R. O. SPRINGER: Yes.

Mr. CHAIRMAN: But to leave it in the cyberbullying, Clause 20.

Dr. R. O. SPRINGER: Probably include emotional distress in there as well.

Mr. CHAIRMAN: No, you have that. You have it.

Dr. R. O. SPRINGER: In Clause 20? I do not see it in Clause 20. Where is it in Clause 20.

Mr. CHAIRMAN: The last one. *"Causes substantial emotional distress…".*

Dr. R. O. SPRINGER: Yes. Yes. Then, I will take out *"embarrassment"*.

Mr. CHAIRMAN: So, you would take out *"embarrassment"*?

Dr. R. O. SPRINGER: I think that covers *"embarrassment"*. *"Emotional distress"* covers a whole range of negative emotions or feelings. *"Embarrassment"* is one (1) such. It is the next level to *"embarrassment"*; the one that really requires that intervention by the law.

Mr. CHAIRMAN: The DPP felt *"embarrassment"* could stay in Clause 20 but for Clause 19, it is too vague. My thinking was that it either comes out of both or stays in both. What do other Members think? Any Members have an opinion? Honourable Opposition Leader, you wish to make a comment on it?

Mr. R. A. THORNE: No, thanks.

Mr. CLERK: Mr. Chairman, just to be clear, the *"embarrassment"* was in Clause 19 before?

Mr. CHAIRMAN: Look at the Bill as originally drafted.

Mr. CLERK: I am looking at it now.

Mr. CHAIRMAN: It was in or it was not?

Mr. CLERK: Yes. It was in Clause 19(3).

Mr. CHAIRMAN: Right.

Mr. CLERK: It was not in Clause 19(2) but it was in Clause 19(3).

Mr. CHAIRMAN: Yes. Can we maintain it in the cyberbullying, but omit in Clause 19?

Dr. R. O. SPRINGER: Mr. Chairman, I believe it should be omitted from Clause 20, as it

has already been omitted from Clause 19. I think that is captured in *"substantial emotional distress"*.

Mr. CHAIRMAN: Honourable Mr. Phillips, what is your opinion?

Mr. P. R. PHILLIPS: Mr. Chairman, I am of the view that it is either in both or not in any.

Mr. CHAIRMAN: Senator Nurse; Senator Walters, any opinion?

Senator R. O. WALTERS: No opinion, Mr. Chairman.

Senator the Hon. L. E. NURSE: I would be inclined to take it out.

Mr. CHAIRMAN: You would be inclined to take it out, Senator Nurse? Out of both?

Senator the Hon. L. E. NURSE: Both Clauses 19 and 20.

Mr. CHAIRMAN: Okay. Just forebear with me a bit. Senator Nicholls, remember of course but he said he would still be available.

Asides.

Mr. CHAIRMAN: Just for the record Senator Nicholls agrees with me to leave it in both. I do not know. My proposal would be to leave it in.

Mr. CLERK: Mr. Chairman, just for the record…

Mr. CHAIRMAN: That he (Senator Nicholls) cannot … because he is not present. I know. I know. My proposal would be to leave it in and let a court decide whether that word is too broad or not because a court could sever…

Dr. R. O. SPRINGER: Mr. Chairman, not that I question the legal minds like yourself and Senator Nicholls but we all have questions as it relates to the word. I mean, someone laughs at you and you become embarrassed. You misspeak and someone mentions it and you become embarrassed or you could be embarrassed because of that. No. It is too vague a word for too many reasons and too many things that are not even criminal you could be embarrassed.

If someone creates a little meme about you on social media that is embarrassing but it may be embarrassing for a day or two (2) but soon it is forgotten. I do not think a person should be hauled before the courts for something as trivial as that. If someone does something that causes you to seek medical intervention; you have to go to a psychiatrist or counselling or such like, that is substantial emotional distress. For that, I believe a person should be hauled before the law courts.

Mr. CHAIRMAN: It is a complex issue. I agree with you.

Dr. R. O. SPRINGER: Not for embarrassment …

Mr. CHAIRMAN: It is a complex issue. Recognise that the word was left in, as I said, under advisement by the experts at the Budapest Convention and the Europeans in other languages.

Dr. R. O. SPRINGER: Perhaps, culturally, embarrassment means more to them than to us.

Mr. CHAIRMAN: Well, it is in other legislations in the Caribbean.

Dr. R. O. SPRINGER: But that does not mean we have to keep it if we agree here in this Committee that it is a bit too vague.

Mr. CHAIRMAN: Mr. Clerk, what happens? I mean because the Senate does not have to accept our proposal right? Clearly because we cannot be the final adjudicator on this.

Mr. CLERK: Well, neither the Senate nor the House has to agree on any amendments that you have made but if the Committee recommends them; it is up to the Senate then to decide whether it will go in a different direction. Similarly, they (Senators) may go in a different direction in relation to the same, the varying levels of punishment and fines that were recommended in Clauses 19 and 20.

Mr. CHAIRMAN: Dr. Springer, I am minded to leave it in and let those higher up but…

Mr. CLERK: But Mr. Chairman, you may have to put it to the vote since you have Members here who are saying to take it out; you then cannot leave it in.

Mr. CHAIRMAN: So you want me to put it to a vote?

Mr. CLERK: You went around the table and certainly based on what was said, the majority seemed to …

Mr. CHAIRMAN: No. Let us take a vote. Those who feel it should be taken out, say 'Yes'. Mr. Phillips what about you? Do you feel it should be taken out from both Clauses 19 and 20?

Mr. P. R. PHILLIPS: I agree Sir. Take it out!

Mr. CHAIRMAN: Senator Nurse. You would take out the word *"embarrassment"* out of both Clauses 19 and 20?

Senator the Hon. L. E. NURSE: Yes. I would be inclined to take them out.

Mr. CHAIRMAN: Alright

Mr. CLERK: Leader of the Opposition?

Mr. R. A. THORNE: I do not know that you should criminalise *embarrassment* so.

Mr. CHAIRMAN: Okay. Senator Walters?

Mr. R. A. THORNE: Sorry Ryan and my view is not restricted to the word *"embarrassment"*. I have difficulty with other words in here but you are asking about *"embarrassment",* but I just wanted to make that clear.

Senator R. O. WALTERS: I was actually going to make that point about the other words in there because this Section is one of the sections that came up very often with those persons that presented objections to the Bill and based on what is being presented; it has not substantially changed.

I think that that is something that the Committee has to review or should at least discuss. *"Humiliation"* is a similar word to *"embarrassment"*. *Anxiety* is subjective so I am just saying it needs a little more discussion in terms of the context of the whole section and those emotive words that have been used.

Mr. CHAIRMAN: Alright so…

Mr. CLERK: In relation to *"embarrassment"*, what is your vote?

Senator R. O. WALTERS: Similar. It should not be included. In other words, we do not believe it should be included, either.

Mr. CLERK: We can discuss the other words but…

Mr. CHAIRMAN: *"Embarrassment".* So, five (5) Members as opposed to me, one (1), who feels that we can leave it in; so the vote is for it to be removed.

In terms of further discussion on Clauses 20 and 19 as proposed, as before us now amended, you said Senator Walters, you felt that there should be other words removed. When all is said and done, you might say the entire section should be removed period, and these are some of the core sections of this Bill. Do we want a Cybercrime Bill or not?

Senator R. O. WALTERS: What I am saying though, is that the Committee was charged with hearing the views of the public and presentations from each of them and out of the persons that presented, I believe maybe one (1) of them, Mr. Williams, was more friendly to the words in the Bill.

I am saying if you have presented an opportunity for persons and the majority of those persons have displayed displeasure or a grievance with some of the wording in some of the sections I think that we should consider re-wording, instead of poking at words, the context in which some of the sections, especially maybe 19 and 20, are laid out to give more comfort. That is all I am saying.

It may not be a situation of poking at words but how it is worded and what it is really intended to do.

Mr. CHAIRMAN: What is your proposal, having said that? What is your proposal? How would you word this 19 and 20 having said that? The Committee has agreed to take out *"embarrassment"* now from it. We have taken out the words "*ridicule and contempt".* As I said, the question is whether this Committee is saying forget about Section 19 and 20 because we have now taken out, as I said, *"ridicule"; w*e have taken out *"contempt"* and we have taken out *"embarrassment"*, so in my opinion to take out more words now means that you could as well not add these sections and let people say anything they want to say about you.

They could call you a homosexual; they could call your mother a whore; they could say that you have this or that, you have Acquired Immunodeficiency Syndrome (AIDS). What purpose are we serving?

I say things are alright and remember, I asked Mr. Kemar Stuart this directly. He might have felt a bit offset that people want the right to be able to say anything about people, whether it is people in public life or not, with impunity under the under the limb that it is freedom of expression or freedom of speech but yet when it comes to them, they do not like it. I do not know.

I certainly have suffered at the hands of an individual who said all kinds of things that went globally about me, that could have cost me a lot but for the fact that people who cared about me, have a big mind as well too. That is why I am asking, do we want a Bill or not? Do we want a Bill or not because it is all well and good that the same people who came in before us and made those criticisms … if somebody were to tell them something about their mother they would want to kill or beat them. Senator Walters?

Do not let us talk in broad terms, let us be specific. What would you like to see? I think we have made a lot of concessions here by taking out "ridicule", "contempt" and "embarrassment" by saying that the words have to be false whilst before in Section 19(3), it was whether you do not care whether they are true or false; in substituting

that the words must be *false*. I believe concessions have been made to put before The Senate. As I said, The Senate and the Lower House, we are just a committee of those Chambers, can choose to disagree and to choose to go along with you, that further amendments are to be made or not.

There is no perfect legislation. There never will be when it comes to trying to order human behaviour and my view is to leave it as is, and carry on. Are there any other amendments from what is before us as amended that you would wish to make?

If there are no others, I think, we would move on. Section 23 as amended, we had to put in the judge or magistrate. That was a clear omission from the Bill as presently drafted that went before both Houses of Parliament. The final amendment which we requested and which, as I said, is back up for consideration is on Section 23, where we asked about putting in the issue of privileged information on material protection, based on the concern from the Bankers' Association. That Clause, or protection within the context of the Proceeds and Instrumentalities of Crime Act, is within the context of Barbados Revenue Authority (BRA) information from …

Mr. CLERK: Sir. Sorry, you mentioned judge or magistrate but there was also another amendment too. It was in Section 23(2) which we did not look at.

Mr. CHAIRMAN: We are dealing with Section 23 now.

Mr. CLERK: But you started at Section 23(1) and then you are all down at 23(6) but there is one (1) at 23(2). I am just letting you know.

Mr. CHAIRMAN: Do you mean "*or contains evidence*"?

Mr. CLERK: Yes.

Mr. CHAIRMAN: I think we had asked for that.

Mr. CLERK: Yes. I just wanted to be completely...

Mr. CHAIRMAN: Does anyone have any issues with putting in "or contains evidence"? I think that was put in for clarity's sake to avoid the charge being not grounded because of the technicality.

On the issue of the privileged information, as I was saying, under the Proceeds and Instrumentalities of Crime Act, I know that that privileged information, when you look at it, relates to information from the Barbados Revenue Authority (BRA).

How the Office of the Chief Parliamentary Counsel (CPC) drafted this privileged information issue is attorney-client privilege, essentially. Attorney-client privilege, is established, an anciently granted right and I am not so sure that how this is drafted at all reflects any exception of privileged information or material where it already exists. I would propose omitting this because it does not add anything to existing convention. How do Members feel about that? Any opinions anyone? I said ultimately too, I mean as I think it was agreed to by the Chief Parliamentary Counsel (CPC) as well, it is an issue or policy decision that would have to be made. I believe the point can be noted and when it reaches the Houses of Parliament, if on an issue of policy, people wish to put in a privileged information exception – which may be wider than the attorney-at-law/client privilege as well – they will be free to do so. Do Members have any opinion on this either way?

Asides.

Mr. CHAIRMAN: Mr. Clerk, note that we have again put it back as was originally sent, as an issue of policy as to whether that should be in, but go back to the original where it is not included. Are there any other aspects of the Bill as amended before us that anyone would wish to raise? Clearly, this is a section where you have to get the court order anyway, so there is judicial discretion as to whether to grant an order for disclosure or not. Again, I believe we should just leave it to the judge or presiding officer to decide whether the information should be disclosed or not. If there are no other issues with the Bill as amended, can we go on to Item five (5): Composition of the Report? Clerk of Parliament, I believe that these reports take a set format, so do you want to go through to see if we agree?

Mr. CLERK: Yes, Mr. Chairman. We have started on the report and essentially on the first page we have indicated that when the Senate would have committed these Bills to the Joint Select Committee (Standing), you have the membership of the Committee; the Terms of Reference that were approved. The Committee would also have indicated the number of meetings that it would have held.

The Minutes of those meetings are attached. We basically would have set out exactly what the

Committee decided in terms of the persons and organisations which we would have received submissions from; all of that is included in the report. The list of persons from whom we actually received written submissions as well, which would show that we had some 47 written submissions. Those would be appended to the report. The Committee ordinarily would have gone through the entire 47 written submissions but I do not think we did that.

We took out the main ones which amounted to about six (6) or seven (7) and then there were persons who had indicated that they would prefer and requested to make oral presentations. Those will also be included and the Committee's interaction with those oral presenters. I think the Committee had determined at one (1) of its earlier meetings that in relation to those other submissions, the Clerk would do a brief and succinct summary of the points that would have been raised in those submissions.

We had started to do that and that will be included in the report. The interaction between the Committee and those Members who presented orally will also be included in the report. The examination of both Bills will be included and the examination of obviously the amended Bill will be included in the report. Then we will have the conclusion and the acknowledgement. That will essentially be the format that we will use.

Mr. CHAIRMAN: What about the inclusion of the legislation from other Caribbean countries?

Mr. CLERK: We can. Once the Committee determines that; we will put them in.

Mr. CHAIRMAN: Yes, I would want that in, plus the Jamaica Prosecution Guidelines.

Mr. CLERK: Once the Committee determines that, we will put them in, Sir.

Mr. CHAIRMAN: I would want that in, plus the Jamaica prosecution guidelines as an *aide-memoire* for us, which was sent.

Mr. CLERK: Do you have those?

Mr. CHAIRMAN: Yes, I sent them to you all. I can resend.

Mr. CLERK: We will include them then.

Mr. CHAIRMAN: Yes, and the submissions would include those that came in after the deadline that we agreed to, like the BAR Association; the Bankers and the Director of Public Prosecution (DPP). Okay, is there anything else which any other Member believes should be in?

Mr. CLERK: Sir, obviously we have to then send the amended Bill back to the CPC to have it further amended, and we would then circulate that too.

Mr. CHAIRMAN: The deadline is now what from the Senate? 07 August,**2024**? Okay. You said Parliament has started to work on the report so, barring unforeseen circumstances like this week, where we lost two (2) days – those things are not at all within anyone's control – and barring that kind of eventuality, when do you feel we can have everything finalised?

Mr. CLERK: End of July, **2024**, Mr. Chairman.

ADJOURNMENT

Mr. CHAIRMAN: Just before **Kadooment** weekend. Okay, Members is there Any Other Business? If none, I entertain a motion for an adjournment *sine die*.

Mr. P. R. PHILLIPS: Mr. Chairman, I beg to move that this sitting be adjourned *sine die*.

Dr. R. O. SPRINGER: I beg to second that.

The question was put and resolved in the affirmative without division.

Mr. CHAIRMAN: I believe we have some light refreshments as usual in the Members' Room.

Thank you all for coming and let us continue to thank God for life and pray that we are spared the harsh effects of the adverse weather conditions. We pray for sister CARICOM countries that have been more affected by **Hurricane Beryl**. Thank you.

REPORT OF THE JOINT SELECT COMMITTEE (STANDING) ON GOVERNANCE AND POLICY MATTERS ON THE CYBERCRIME BILL, 2024 AND THE MUTUAL ASSISTANCE IN CRIMINAL MATTERS (AMENDMENT) BILL, 2024