Houses of Parliament
Jamaica

REPORT OF THE JOINT SELECT COMMITTEE APPOINTED TO REVIEW AND REPORT ON "THE CYBERCRIMES ACT, 2015"

1. ESTABLISHMENT, COMPOSITION AND TERMS OF REFERENCE OF THE COMMITTEE

Members of this Honourable House are reminded that on the 12th day of January, 2021, the Hon. Daryl Vaz, MP, Minister of Science, Energy and Technology, having obtained suspension of the Standing Orders, moved:

WHEREAS section 25 of the Cybercrimes Act 2015 provides that the provisions of the Act shall be reviewed by a Joint Select Committee of the Houses of Parliament three years from its date of commencement;

AND WHEREAS the commencement date of the Act was December 22, 2015:

BE IT RESOLVED that, notwithstanding Standing Order 76(1), this Honourable House of Representatives appoint a Special Select Committee comprising the following Members:

Hon. Daryl Vaz – Chairman
Hon. Floyd Green
Hon. Alando Terrelonge
Hon. Robert Nesta Morgan
Ms Tamika Davis
Ms Kerensia Morrison
Mr Franklin Witter
Mr Julian Robinson
Mr Hugh Graham

to sit jointly with a similar Committee to be appointed by the Senate, to review and report on "The Cybercrimes Act, 2015".

Members are further reminded that on the 15th day of January, 2021, the Hon. Kamina Johnson Smith, Minister of Foreign Affairs and Foreign Trade, having obtained suspension of the Standing Orders, moved:

BE IT RESOLVED that this Honourable Senate appoint a Select Committee comprising the following Members:

Senator the Honourable Matthew Samuda
Senator Kavan Gayle, CD
Senator Dr. Saphire Longmore
Senator Natalie Campbell Rodriques
Senator Peter Bunting

Senator Gabriela Morris

to sit jointly with a similar Committee appointed by the House of Representatives to complete the statutory review of the Cybercrimes Act.

Members are reminded that on the 30th day of March, 2021, the Hon. Edmund Bartlett, Minister of Tourism and Leader of the House moved a motion enabling the Committee to hold virtual meetings, whether wholly virtual or partly virtual and partly physical, utilizing available information and communications technologies.

Members are further reminded that on the 22nd day of April, 2022, Senator the Honourable Matthew Samuda, Minister without Portfolio in the Ministry of Economic Growth and Job Creation, having obtained suspension of the Standing Orders, moved:

BE IT RESOLVED, with reference to the resolution approved by this Honourable Senate on the 15th day of January, 2021, appointing a Special Select Committee to sit jointly with a similar Committee appointed by the House of Representatives to conduct the statutory review of the Cybercrimes Act, that the name "Sherene Golding Campbell" be added thereto.

Members are also reminded that by virtue of a resolution approved by this Honourable House on the 7th day of February, 2023, the composition of your Committee, as set out above, was made to continue in force for this Session of Parliament and we were empowered to proceed with matters that were before us from the stage reached at prorogation.

A similar motion was approved in the Senate on the 10th day of February, 2023.

2. INTRODUCTION

In keeping with the statutory requirement of the *Cybercrimes Act, 2015* ("the Act"), your Committee started its review on the 24th day of March, 2021. We agreed at our first meeting that we would take a consultative approach by inviting members of the public, through public notices placed in the major newspapers, to make submissions on the Act, as well as writing to specific entities inviting them to make submissions. The notices were placed in the Sunday Observer and the Sunday Gleaner on the 28th day of March, 2021 and on the 25th day of April, 2021.

Some of the entities that we sought views from did not respond to your Committee's request.

We received and heard submissions from the following entities:

- Jamaica Cyber Incident Response Team (JaCIRT), Ministry of Science, Energy and Technology (MSET)
- Major Organised Crime and Anti-Corruption Agency (MOCA)
- Ministry of Education, Youth and Information (currently the Ministry of Education and Youth (MOEY))
- Joint submission from the Ministry of National Security (MNS) and the Communications Forensics and Cybercrime Division (CFCD)

- Office of the Director of Public Prosecutions (ODPP), Ministry of Justice (MOJ)
- Joint submission from the Private Sector Organisation of Jamaica and the Jamaica Technology and Digital Alliance
- Financial Services Commission (FSC)
- Department of Computing, The University of the West Indies
- University of Technology, Jamaica
- Jamaica Bankers Association
- Symptai Consulting Limited

The technical team that assisted your Committee in its deliberations comprised of representatives from:

- MSET
- Office of the Parliamentary Counsel (OPC)
- Attorney General's Chambers (AGC)
- Legal Reform Department (LRD)

We held a total of twenty-one (21) meetings, the last being on the 19th day of April, 2023 (***See Appendix II***). With the exception of our first meeting, all meetings were held virtually using the Zoom platform. A caucus was held on April 13, 2022, which was an informal meeting to discuss the way forward in examining the provisions of the Act. At this informal meeting, the MSET made a presentation on sections 10 and 11 of the Matrix of submissions. The decisions that were made at this informal meeting were ratified at a formal meeting held on April 21, 2022.

Your Committee now has the honour to presents its findings and recommendations.

3. General Observations

We noted from the submissions received by your Committee that stakeholders generally accepted the importance of the Act in addressing cybercrime, but noted concerns relating to some of the provisions, particularly the offences provisions. Some general issues that were raised and discussed by Members of your Committee were cyber incidents, malicious communications, willful intent, and the extraterritorial reach of the Act.

Cyber incidents

Your Committee noted that the challenges in cyberspace evolve daily. We were informed by JaCIRT that the top three categories of reported cyber incidents were abusive content, impersonation, and revenge porn. The entity advised us that there were over 136 reported incidents in 2020, and one of the challenges it faced was that a number of reported incidents were not followed through to prosecution. We took note that more than 70% of the 136 cases were referred to the CFCD as they were deemed to be prosecutable based on the nature of the offence reported. In terms of the number of cybercrime matters placed before the Parish Courts from 2017 to 2020, data from the ODPP revealed that for 2017, there were 65 active cases, six inactive cases and 26 cases that were disposed. In 2018, there were 61 active cases, two inactive

cases and 12 cases that were disposed. In 2019 and 2020, a total of 83 new cases were filed, 103 cases were disposed, and 107 cases were pending.

At one of your Committee's deliberations, we discussed a cyber-fraud incident that took place at a financial institution in the country. We were informed that the issue was a phishing campaign where fraudsters sent emails to customers that resembled authentic emails, as well as made calls to customers soliciting their RSA tokens in order to access their bank accounts. Although the specificity of the incident was not known and was the subject of the institution's internal investigations, we saw the relevance of examining this incident by considering if there were provisions in the Act to address same and what was the success rate of investigations of these incidents. We were advised that the Act was able to address the matter, but noted that the details of the investigations would not be made known in the public domain as financial institutions generally dealt with same internally. Members of your Committee expressed the view that because of the approach taken by financial institutions in handling these cases, it may not allow for an adequate assessment of the scale of the issue and the success rate for prosecution was not as great as it should be. **We therefore recommend that there should be an obligation on financial institutions to report, even in an anonymous manner, to the Bank of Jamaica, the aggregate number of cyber-fraud cases. We further believe that the Bank of Jamaica and the FSC should collect data relating to these cases and make it available to law enforcement agencies and the public on an aggregate basis.**

During your Committee deliberations, we were informed of the different types of social engineering attack tactics such as phishing, and were assured by the members of the technical team that in addition to sections 3, 5, 7 and 8 of the Act, sections 3 and 19 of the *Law Reform (Fraudulent Transactions)(Special Provisions)* Act, and section 35 of the *Larceny Act* covered same since these activities were generally preparatory to the commission of a fraudulent activity.

Malicious communications

We expressed concern about the attack on a person's reputation in cyberspace. We felt that a line should be drawn between free speech, where a person expresses disapproval or dislike for someone or something, and speech made that would place a person's life, career and income at risk. One stakeholder advised your Committee that an offence that constituted defamatory comments should be addressed by the civil court as a neutral arbiter instead of a criminal court, and that an injunctive relief could be sought. We expressed reservation regarding the comments. **We note that section 9 of the Act covers the offence of malicious communication and therefore recommend that the ODPP's *Guidelines for Prosecuting Cases involving Malicious Communications: Section 9 of the Cybercrimes Act of Jamaica, 2015* be included in any public education campaign to address the matter of malicious communication. We are of the view that the Jamaica Constabulary Force should be aware of same in dealing with certain cases.**

Wilful intent

We noted in our review of the Act that some stakeholders recommended that for some of the offence provisions, consideration be given to persons who act with intent or wilfully. We were advised that legislation generally apply the mental element of intent and no cybercrime legislation was identified that introduced the mental element of "recklessness".

Extraterritorial reach of the Act

Having learnt that it was difficult to prevent transborder cyber incidents, we questioned whether the Act provides an extraterritorial reach. One stakeholder also pointed out that there was no reference to extradition of nationals if overseas authorities traced illegal activities to Jamaican nationals. Members of your Committee were advised by the MSET that the *Extradition Act* provides for the extradition of nationals. We learnt that it was not the intention of section 22 of the Act to address acts committed outside the jurisdiction using a computer. We, however, noted that there were bilateral and multilateral agreements that facilitated cooperation, and under the auspices of the Organization of American States, there are Computer Security Incident Response Teams of the Americas in countries such as Canada, the United States of America, and countries in Latin America, South America and the Caribbean. Where a matter involved a national of another country, the Ministry of Foreign Affairs and Foreign Trade and MOCA, through agreement with law enforcement agencies in that country, could make representation. We were advised that despite the fact that Jamaica is not a party to the Budapest Convention on Cybercrime ("Convention"), the offences in the Act are guided by same. It was noted that the Convention makes provision for the extradition of persons between party countries for criminal offences punishable in the legislation of both States.

We noted the importance of respective entities in the national cyber ecosystem, namely, the Office of the Cabinet, the National Security Council, the Cyber Intelligence and Incident Response branch of the MNS, the CFCD, the MOCA, the JaCIRT, and the ODPP.

4. FINDINGS AND RECOMMENDATIONS

A. Specific Recommendations

Part I- *Preliminary*

Section 1 – Short title

Your Committee recommends that no amendment is necessary for this section.

Section 2- Interpretation

This section provides the interpretation to key terms that are used throughout the legislation. Based on concerns raised by stakeholders, your Committee wishes to make the following recommendations:

"computer"

We questioned if the internet of things was covered in the definition of the term "computer". Members of your Committee were informed that the internet of things was considered in like form to a computer system in cybercrime and cybersecurity legislation. We noted that the reason for same was that devices connected to the internet were susceptible to the same type of activities that cybercriminals perpetrate against computer systems.

One stakeholder suggested that clarity should be provided on whether the Act intends to cover only crimes over a "network" or crimes committed using an electronic device generally. The stakeholder also recommended that a definition be included for "data storage device". Your Committee was advised that the Act intends to cover crimes committed against or using a computer, whether the computer is a standalone device or part of a network, as articulated in sections 3 to 9 of the Act. Regarding the inclusion of a definition for the term "data storage device", we were advised by the MSET that although the term or a variation of the term was defined in some cybercrimes legislation in other countries, there was no need to define same in the Act since the definitions of terms such as "computer", "data", "electronic", and "electronic communications system" inherently provided for electronic devices that stored data.

Your Committee recommends that no amendment is necessary for the definition.

"damages"

We noted the suggestion of some stakeholders that the term "damage" should be expanded to include different types of damages such as psychological injury and mental injury/distress. In our deliberations, your Committee considered whether to include the term "mental injury" or "psychological injury" in the definition. One Member of your Committee expressed the view that the term "mental injury" should be used in the definition since mental health encompassed all psychological-related issues, but psychological injury might not encompass all possible mental health components. The LRD advised your Committee that the court has viewed "mental injury" as a psychiatric illness in civil litigation. It was noted that the term was only defined in section 27 of the New Zealand Accident Compensation Act, 2001, as a *clinically significant behavioural, cognitive, and psychological function*. Members of your Committee were advised that based on case law, it was found that mental injury was considered as *a disturbance of the mind that is serious and prolonged and rises above the ordinary annoyances, anxieties and fears that come with living in civil society and need not be proved by medical evidence*. On the other hand, psychological injury or harm was considered an aggravating factor in determining the appropriate custodial sentence, and the court could make inferences based on information contained in a social inquiry report including statements from the victim. Your Committee learned that the courts considered mental injury or harm as a recognized psychiatric illness.

Having considered the issues, we agree that the term to be considered in the provision should be carefully decided since it would have implications on how the offence would be

prosecuted. We support the view that there should be wide consultation among medical, legal, judicial and academic experts to resolve the issue of the type of injury that would be appropriate for inclusion in the Act and that the term be defined once a decision is made based on the preferred definition. We recommend that the Ministry of Health and Wellness consider amending the *Mental Health Act*.

"function"

We noted the recommendation from one stakeholder that the definition should include "addition" and "modification" given that the term "deletion" was provided for in the definition. The MSET team advised us of nine jurisdictions and their cybercrimes legislation, and indicated that five of them did not define the term "function" although the term was used in their legislation. The team further pointed out that the other four countries defined the term in the same way as it was defined in the Act. We were informed that no evidence had been found where the term "function" was defined to make specific reference to "addition" and "modification". However, the use of the word "includes" suggest that the term was not limited to the terms referenced in the definition.

Your Committee recommends that no amendment is necessary for the definition.

"key"

Your Committee noted the typographical error in the definition of the term "key", **and recommends that the word "date" be changed to the word "data". We also recommend that the term should be defined to make reference to electronic and digital keys.**

Section 2(2)

"access"

Your Committee did not accept a recommendation that was made by one stakeholder to amend the definition of "access" to include the words "any function that willfully and knowingly initiates" as the offences to which the use of the term "access" relate articulate the requisite *mens rea* of intent. We also did not accept a recommendation to amend section 2(2)(a) to include the word "create" as we were advised that in the context of cybersecurity or information security, one could not simply "create" anything, one simply adds to an existing dataset or framework. It was noted that the term "alter" sufficiently covered the concept of creation or modification.

One stakeholder expressed the view that the word "storage" was used throughout the Act and it was unclear what was meant by the term. It was suggested that the term should be defined. We observed that the term was used in section 2(2)(b). **We are of the view that the word should not be defined since it is used throughout the Act in the context of other terms that are referenced in relation to a computer.**

One of the issues raised by Members of your Committee was how persons who found vulnerabilities in a system, and reported same, would be treated. The MSET advised your Committee that the unwitting discovery of vulnerabilities should be separated in two categories. The first would be a person who discovered vulnerabilities as part of their job function, and the second, a person, who, without the knowledge or authority of the owner, "broke" into internet facing resources. The first category would be indemnified by the terms of their employment and there was no penalty for same under the Act. On the other hand, where acknowledgment and approval were not gained from the owner of the resources, even if the person or persons were legitimately carrying out security research against resources, they would be guilty of an offence. Therefore, the Act does not criminalize white hat hacking or security research done within a structured framework with the necessary approvals.

Your Committee recommends that no amendment is necessary for the definition.

Part II – *Offences*

Section 3 – Unauthorised access to computer program or data

Some Members of your Committee expressed support for the recommendation of one stakeholder that a framework be provided in the Act to recognize ethical hackers, and that Standard 7, which is found in section 30 of the *Data Protection Act, 2020*, be considered. We were advised that accessing a computer system without authorization would threaten the integrity of a computer system. Therefore, the criminalization of illegal access represented an important deterrent to many other subsequent acts against confidentiality, integrity, and the availability of computer systems. The MSET advised your Committee that Standard 7 provides that the appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing and accidental loss or destruction of, or damage to, personal data. It further provides that measures should be taken to ensure that the Information Commissioner is notified, without undue delay, of a breach of the data controller's security measures which might affect personal data. Also, the Standard provides guidance on the types of technical and organisational measures that could be taken and the requirements that must be met where processing is carried out by a data processer on behalf of a data controller. Members of your Committee were advised that section 45 of the *Data Protection Act, 2020,* places an obligation on a data controller to annually submit a data protection impact assessment outlining, among others things, the measures envisaged to address risks including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the *Data Protection Act, 2020.* It was noted that section 30(8)(A) of the *Data Protection Act, 2020*, is limited in nature and provides a defence in instances where a person wilfully and without lawful authority breached any pseudonymization or encryption applied to any personal data, which was specific in the defence of public interest. After careful consideration, we support the advice of the MSET that to access a computer system without authorization would be tantamount to accessing private property. **However, we are of the view that policy options around the broader**

concept of ethical hacking, which would include grey hat hackers and persons who genuinely search networks to determine vulnerabilities and indicate same, be examined.

It was noted that whilst there is no formal arrangement outlined in any legislation for reporting the vulnerability of a computer system, reporting could be done through JaCIRT. It was noted that JaCIRT would ensure that messages are delivered through a third party to the owners of a network for the necessary actions to be taken to mitigate challenges identified.

Your Committee recommends that no amendment is necessary for this section.

Section 4 – Access with intent to commit or facilitate commission of offence
It was recommended that section 4(1) be amended to state that a person commits an offence if he or she accessed or caused to be accessed any program or data. It was revealed that the intention of the proposed amendment was to ensure that the provision captured a person who did not directly access any program or data held in a computer, but facilitated the access by a third party. The MSET team informed your Committee that section 12 of the legislation treats with the matter of inciting and conspiring with another person to commit an offence under the Act, and did not see the need to amend the provision to take into consideration the recommendation. **We support the view expressed by the MSET.**

One stakeholder expressed the view that the section should be amended to provide for harsher penalties where the offence relates to a child, and that the penalties under sections 4 and 5 of the *Child Pornography (Prevention) Act* should be considered. It was further recommended that since cybercrime and child pornography were incorporated in the same legislation in other jurisdictions, the Act should be merged with the *Child Pornography (Prevention) Act* as there were similarities with the provisions of both legislation. **We support the suggestion that there should be harsher penalties in relation to offences against children, and that there should be a distinction between the penalties for offences committed against children by children and adult offenders. We further support the recommendation that the term of imprisonment be increased from 15 to 20 years for an adult who commits an act where the victim is a child.**

We were informed that an obligatory international agreement was fulfilled when the *Child Pornography (Prevention) Act* was enacted, and that a merger of the Act with the *Child Pornography (Prevention) Act* would require policy direction.

Your Committee recommends that no amendment is necessary for this section.

Section 5 – Unauthorised modification of computer program or data
Your Committee recommends that no amendment is necessary for this section.

Section 6 – Unauthorised interception of computer function or service
Your Committee recommends that no amendment is necessary for this section.

Section 7 – Unauthorised obstruction of operation of computer
Your Committee recommends that no amendment is necessary for this section.

Section 8 – Computer related fraud or forgery
It was recommended by one stakeholder that consideration be given to the introduction of an offence or category of offences that treat with the possession, creation, and reproduction of electronic copies of forged documents. We were advised that the forgery of certain documents was considered a felony and attracted custodial sentences for a term of seven years up to life imprisonment, and other documents, if forged, were considered a misdemeanour and attracted a penalty of imprisonment for a term not exceeding two years. **Your Committee, having learned that the *Forgery Act* is technology neutral and treats with certain types of forged document, recommends that amendments be made to that legislation to take into account the creation of an offence generally relating to the possession of forged documents with the intent to defraud or deceive.**

Section 9 – Use of computer for malicious communication
One recommendation that was made to your Committee was the inclusion of "hate speech" as a type of communication deserving of punitive treatment. Your Committee was divided on whether the matter of hate speech should be included in the Act. One Member felt that "hate speech" should not be included at this time because of the varied views on religion, sexuality and ethnicity. Another Member supported the inclusion of "hate speech" because a provision for same would provide the court with the ability to make a determination in particular cases on hate speech. Your Committee was advised that the issue was a question of proportionality between freedom of expression and defamatory offences, and there was no disagreement in principle on "hate speech". We were further advised by the LRD that the issue of hate speech engaged several rights under the Constitution, especially the freedom of expression. It was suggested that the Ministry with responsibility for information should take the lead in crafting provisions on the offence of "hate speech".

The LRD's team agreed with the proposal that "revenge porn" or the sharing of an "intimate image" deserved special treatment under the Act. We were informed that some jurisdictions addressed the proposed offence in a technologically neutral way whereby the form of publication was not limited to computers. It was suggested that the proposal could be included in a new section 9 because it was sufficiently wide in its scope as the provision addressed data published with an intention to harass or to cause harm.

Members of your Committee recommend that the section be amended with consideration being given to the following:

i. **the word "publish" should replace the word "send", and be defined along the following line:**
"publish" in relation to data includes, sending, transferring, posting, disseminating or otherwise providing access to data.

ii. **a new subsection should be inserted to make provision for intimate images. Additionally, the word "obscene" should remain although the view was expressed by a stakeholder that a provision covering intimate images would address same.**

Your Committee expressed concern about the frequent sharing of images of scenes of accidents involving personal injury or death. We noted that the sharing of these images could place the person(s) depicted in the images, their family and others, in distress. We questioned if the sharing of these images would be addressed by the Act, and if not, whether a provision could be inserted in the Act to address same. After careful consideration, we noted that section 9(1) of the Act would address the issue, but the intent to harass, cause harm, or the apprehension of harm would have to be proven. We were also guided by the ODPP's *Guidelines for prosecuting cases involving malicious communication* on the said section. We noted that if the intent could not be proven, the person affected would need to pursue a civil lawsuit. We were assured by the MSET that along with the Office of the Information Commissioner, it will engage in a public awareness campaign on the *Data Protection Act, 2020* to sensitize persons about the processing of data that are of a personal nature. **We recommend that the public education campaign to be considered by the MSET should include contents that will assist to dissuade persons from the practice of sharing these types of images. We further recommend that there should be discussion with the police and the ODPP regarding the section and how it could be used to address cases reported by citizens.**

Section 10 – Unlawfully making available devices or data for commission of offence
We endorse the MSET's proposal that the section be amended to bring it in line with the Convention by providing that an offence is committed if a person, without unlawful justification, intentionally:
i) manufactures, sells, imports, distributes, discloses, or otherwise makes available:
(a) a computer;
(b) any key; or
(c) any other data or device,
that is designed or adapted primarily for the purpose of committing an offence under any of sections 3 to 9; or

ii) receives or possesses an item mentioned in subparagraph (a), (b) or (c) with the intent that it be used by any person for the purpose of committing an offence under any of sections 3 to 9.

Section 11 – Offences relating to protected computers
We accept the recommendation of one stakeholder that the section be amended to include protected computer systems that are necessary for, or used directly in connection with revenue services.

We recommend that the word "medical" in section 11(2)(e) be changed to the word "health" as we believe that the term is broader to cover all health systems.

Section 12 – Inciting, *etc.*
Your Committee recommends that no amendment is necessary for this section.

Section 13 – Offences prejudicing investigation
One stakeholder noted that the burden of proof seemed to be on the person against whom the charge is laid. The stakeholder stated that the level of evidence required to ground an offence of this nature should meet the standard for criminal liability and the burden of proof should not be shifted on the person being accused to prove his innocence. The AGC advised that there was an arguable basis to conclude that section 13 of the Act imposes a burden on the accused to establish a defence, but the burden arises if the prosecution successfully established the core features of the offence. It was further noted that placing the burden on the accused was legally permissible if reasonably imposed and proportionate. We were advised that section 13 of the Act was introduced to mirror provisions of the *Proceeds of Crime Act* after consideration and recommendation by the Joint Select Committee that reviewed the Cybercrimes Act, 2010. As such, the AGC expressed the view that section 13 of the Act was reasonably imposed, proportionate and was legally permissible.

Your Committee recommends that no amendment is necessary for this section.

Section 14 – Offences by bodies corporate
One stakeholder noted that the section relates to offences committed by a body corporate and the relevant sanctions to be imposed. The stakeholder pointed out that the Act seeks to impose strict liability on specified officers. It was recommended that liability be imposed on an employee in circumstances where the employee uses a company's computer or data storage medium for personal use, and that the due diligence required of a corporation should be clear to ensure that liability will not be attached to certain officers. The LRD advised Members of your Committee that if an employee went on a frolic of his own, the employee would be prosecuted similar to any other individual who commits an offence. Research done by the LRD revealed that it was not evident in other jurisdictions where due diligence has been specifically defined so that a company understands its obligations in relation to cybercrime. We were advised that from company law perspective, due diligence on the part of specified officers required them to act in the best interest of their company. The LRD highlighted that the *Data Protection Act, 2020,* requires all data controllers to have measures in place to ensure that their systems are protected. It therefore did not support the recommendation regarding due diligence since the type of responsibility has always been left general so that specified officers were required to ensure the best interest of their companies and the preservation of stakeholders' interests.

Your Committee recommends that no amendment is necessary for this section.

Section 15 - Compensation

In considering the recommendation of one stakeholder that the section should be more definitive to allow compensation to be ordered as a matter of course and not only at the discretion of the Court or on the application of the complainant, **we recommend that the provision be amended to carve out a regime similar to section 24A of the *Criminal Justice (Administration) (Amendment) Act, 2018*.**

Part III- investigations

Section 16 – Interpretation and scope of Part III

One stakeholder noted that notwithstanding section 16(1)(b)(ii), the Act does not provide law enforcement agencies with a mechanism on how they may seek to legitimately render data inaccessible or remove it from a device. The stakeholder pointed out that where a part of the evidence relied on by the Crown included material obtained from a device, law enforcement agencies would be obliged to return the device and any property seized during the course of investigation upon the acquittal of the person. The stakeholder also expressed the view that there was no power available to law enforcement agencies to allow them to permanently erase offending material from the device prior to its return. The stakeholder therefore recommended to your Committee that the categories of data to be sanctioned should be identified or defined. We noted from the AGC's advice that section 16(1)(b) describes the three categories of actions to be carried out in order to exercise the power to seize, but does not include the mechanism to guide law enforcement on how to carry out the power to seize. We further noted that the method by which seizure was effected would be left to a constable who executed a warrant subject to any details in the warrant issued by a judge of a Parish Court. Therefore, the AGC pointed out that the Act leaves the mechanism for executing seizure powers to the administrative policies of law enforcement.

In respect of erasing offending material from a device, your Committee was advised that section 20 allows for the forfeiture of computer material in two circumstances. Firstly, as outlined in section 20(2) where a person had been convicted of an offence, among other things. Secondly, as determined by section 20(3) and (4) where a Parish Court judge or a judge of the Supreme Court in Chambers may order the forfeiture of computer material where the requirements in section 20(2) have not been satisfied. The Act therefore provides a mechanism for the forfeiture of seized computer material outside of a criminal conviction.

Your Committee recommends that no amendment is necessary for this section.

Section 17 – Preservation of data

Your Committee recommends that no amendment is necessary for this section.

Section 18 – Search and seizure warrants

We questioned if the section covered situations where the police inadvertently or criminally allowed proprietary data from a company whose machine had been seized to be released. The AGC advised Members of your Committee that as a general principle, in situations where there was a loss to an entity or the person whose information was unlawfully disclosed, the laws in Jamaica provided a mechanism for persons to seek compensation where it had been established that the victim suffered loss.

Your Committee recommends that no amendment is necessary for this section.

Section 19 – Record of seized material

One stakeholder raised concern regarding the time for the execution of warrants for material seized, and pointed out that the term "as soon as possible" was too wide. Research done by the MSET revealed that there was no legislation that specified a timeline for the inventorying of seized material, and other legislation took a similar formulation as the provision in the Act. Based on consultation with the MOCA, it was noted that there needed to be latitude to allow law enforcement officers to prepare a list of items seized or rendered inaccessible. We took note of the fact that law enforcement officers' compilation of a list of items seized depended on a number of factors to include, the size of the data seized and whether the data was in intelligible form. In order to treat with issues relating to the way in which law enforcement agencies carried out their investigations, we learned that it might be useful to amend the legislation to include a provision that standard operating procedures (SOPs) be developed and observed in carrying out these investigations. **We therefore recommend that SOPs should be placed either in the primary or secondary legislation as part of investigative procedures even if they were merely specific guidelines on matters such as the timeframe within which entities should act.**

Section 20 - Forfeiture

The Act empowers the DPP to apply for a forfeiture order and sets out the criteria that must be satisfied by a Parish Court judge or a judge of the Supreme Court in order to make a forfeiture order. MOCA suggested that the category of officers who could make a forfeiture application should be extended to include Clerks of Court. The ODPP advised that an anomaly was created in respect of section 20(2) of the Act. It expressed the view that the provision addresses post-conviction application for the forfeiture of computer material used in the commission of an offence. The ODPP noted that based on the current wording of the provision, it prevents Clerks of Court from making an application for the forfeiture of computer material after a conviction is obtained. We learnt that section 24(2) of the *Dangerous Drug Act* and section 20A (2) of the *Quarries Control Act* empower the prosecution to apply for the forfeiture of the instruments of a crime. The ODPP posited that based on the wording of these provisions, Clerks of Court would be authorized to make a forfeiture application. It was therefore suggested that an amendment be

made to section 20(2) of the Act to make reference to prosecution instead of the Director of Public Prosecutions. We were advised that the reference would enable either a prosecutor in the High Court acting under the authority of the DPP or Clerks of Court in a Parish Court to apply for post-conviction forfeiture. It was suggested that in specified circumstances where seized material was not the subject of a conviction, only the DPP should have the authority to apply for forfeiture at the Parish Court or the High Court since there would be more serious consideration for the forfeiture of items that were not the subject of a conviction. **We endorse the suggestion made by the ODPP.**

Sections 21 to 28
Your Committee recommends that no amendments are necessary for sections 21 to 28.

OTHER RECOMMENDATIONS
Stakeholders raised general concerns and made recommendations that were considered by your Committee and we are pleased to report on the following:

1. Disclosure of a Key for protected computer to an unauthorized person; unauthorized disclosure of password or access code; and unlawful divulging of information: It was recommended that the mere act of disclosing a key should be an offence, and in respect of protected computers, it should be immaterial whether this disclosure could be proven to have been made for the purpose of committing or facilitating the commission of an offence. It was further recommended that a provision be included which makes it an offence to disclose a key in respect of a protected computer to a person who was not authorised to receive the key. Additionally, another stakeholder proposed that unauthorized disclosure of a password or access code and unlawful divulging of information should be offences addressed in the Act. Based on research done by the LRD, it was noted that in all jurisdictions but one, mere disclosure was not an offence, but must be for the purpose of a wrongful gain, an unlawful purpose, to occasion any loss or with the knowledge that the disclosure was likely to cause prejudice to any person. Your Committee noted that it would be unusual for the proposed amendments to be made to the Act.

Your Committee learned that if consideration were given to amending the Act so that the mere disclosure of a password and access code or other means of access to a protected computer was an offence, then provision would need to be made so that a person who lawfully disclosed a password would not be liable for prosecution by virtue of this provision. We were advised that consideration could be given to amending section 10 of the Act so that, in addition to the offence being committed in order to further the commission of another offence, it would be committed in the alternative if the offence was committed for the purpose of any wrongful gain, any unlawful purpose (other than the furtherance of the commission of an offence), to occasion any loss or with the knowledge that the disclosure was likely to cause prejudice to any person. **Your Committee does not recommend that the proposals be adopted.**

2. Use of premises, etc.: We agree that language similar to section 5 of the *Law Reform (Fraudulent Transactions)(special Provisions) Act* be considered for the proposed offence of 'use of premises'.

3. Cyberstalking: Two stakeholders recommended that a provision be inserted in the Act to provide for cyberstalking. One of the stakeholders suggested that the offence should particularly be in respect of cyberstalking of a child. The LRD informed Members of your Committee that in most of the jurisdictions it reviewed, except for Ghana, cyberstalking was usually dealt with in provisions relating to malicious communications, which is found in section 9 of the Act. In light of the information provided, it was recommended to your Committee that there was no need to amend the Act to consider the proposed offence. Additionally, the LRD recommended to your Committee that the issue of cyberstalking should be dealt with in keeping with the recommendations of the Joint Select Committee that reported on the Cybercrimes Act, 2010, and the Joint Select Committee that reviewed the *Sexual Offences Act* along with the *Offences Against the Persons Act*, the *Domestic Violence Act* and the *Child Care and Protection Act*. It was pointed out that the LRD prepared a policy paper dealing with stalking as an offence, and it made recommendations to the MOJ on the legislative options that were available in creating an offence of stalking, whether by way of the enactment of separate legislation or as an amendment to the *Offences Against the Persons Act* and other laws that were likely to be impacted by the creation of the offence of stalking.

4. Making false publication: We agree with the recommendation that the Ministry with responsibility for information should review the policy regarding false publication and fake news, and there should be consultation with the necessary stakeholders for the right approach to be adopted regarding the way in which these matters are addressed.

5. Cybersquatting (cloning): Having been advised that it was not necessary to accept a recommendation made by one of the stakeholders that an offence provision be created for cybersquatting as sections 5 to 8 of the Act addressed the issue, **we, however, agree with the suggestion proposed by the LRD that Jamaica subscribes to the World Intellectual Property Organisation's (WIPO's) dispute resolution services.** It was noted that the WIPO Arbitration and Mediation Centre deals with domain name disputes without the need for litigation.

6. Cyber defamation: Whilst we noted in one of the submissions the suggestion that provision be made in the Act to treat with cyber defamation, **we are recommending that consideration be given to the establishment of a Joint Select Committee to review the *Defamation Act, 2013.***

7. Cyber threat: We recommend that the Ministries with responsibility for the *Towns and Communities Act* and the *Offences Against the Person Act* should make amendments to the

respective legislation to treat with the issue of threats generally, of which cyber threat would be a subset.

8. Dissemination of obscene materials: One stakeholder suggested that the dissemination of obscene materials should be an offence under the Act. We were advised that the *Obscene Publications (Suppression of) Act* and the *Child Pornography (Prevention) Act* would address the offence, and the Act would apply if a computer or a computer network was used to commit an offence under either legislation. However, we took note that the monetary penalty and the term of imprisonment in the *Obscene Publications (Suppression of) Act* were low and needed to be updated. The LRD advised that since the legislation was passed prior to the Constitution, it was saved from constitutional challenge on the basis of potential infringement on the right of freedom of expression and any amendment would remove this right. **We recommend that consideration be given to reviewing the legislation.**

9. Illegal selling/trafficking – cyber-enabled crime: We noted comments provided by a stakeholder that the internet paved the way for the sale of illegal materials and trafficking, and that these forms of trafficking went unchecked because they were carried out under pseudonyms. Whilst there was no proposal made regarding the matter, Members of your Committee were advised that the *Dangerous Drugs Act* and the *Firearms Act* would prosecute offences relating to narcotics and weapons. Based on the language used in both legislation and section 4 of the Act, if cyberspace were used to commit an offence, it could be prosecuted as a cybercrime.

10. Identity theft and data theft: Comments made regarding identity and data theft were noted by your Committee. In respect of identity theft, we noted that there was no provision in the Act to address same, but the matter was addressed in section 10 of the *Law Reform (Fraudulent Transactions)(Special Provisions) Act.* With regard to data theft, sections 3, 5 and 7 of the Act would adequately cover the issue, and section 61 of the *Data Protection Act, 2020* would cover the issue of personal data. Members were advised that depending on the circumstance, data theft could be classified as an unauthorized modification of a computer program or data under section 5, or the unauthorized obstruction of the operation of a computer under section 7 of the Act.

11. Net/Cyber extortion: A stakeholder defined net extortion as *the copying of an individual's or a company's confidential data in order to extort the said company of a large sum of money.* Members of your Committee questioned if the provisions that govern normal extortion would be applicable to extortion done in cyberspace and whether a separate provision would be necessary for same. We were advised by the LRD that the existing provisions for extortion were adequate, and section 4 of the Act would address same if it were done in cyberspace. There were two approaches that were generally taken in relation to cyber extortion, that is, provision for the specific offence in the Act or the reliance on the general provision relating to extortion. It was noted that most jurisdictions have adopted the latter approach. We were advised that since provision was already made for extortion, there was no need to make provision for a specific offence on cyber extortion.

12. Web jacking: Your Committee noted that there was no need to make specific provision for web jacking since the existing provisions of the Act adequately addressed the issue, specifically the offences of unauthorized access, unauthorized obstruction if a person was no longer able to control a website, or possibly, unauthorized modification of a computer program or data.

13. Cyberbullying: It was pointed out by a stakeholder that there appeared to be a gap in the Act and the *Child Pornography (Prevention) Act, 2009* because they did not address the issue of cyberbullying. We were advised by the LRD that depending on the conduct, cyberbullying could be prosecuted as malicious communication, but the difficulty anticipated was the requirement that it be proven that the communication was obscene, constituted a threat, or was menacing in nature. **Given that cyberbullying takes place amongst school children, we suggest that the Ministry with responsibility for the *Education Act* consider making amendments to the legislation and its Regulations similar to the Ontario Education Act on bullying in general and cyberbullying in particular. It is being proposed that instead of criminal actions, disciplinary measures be taken to address the issue of bullying along with the necessary remedy to address the injury.**

14. *Finger Prints Act*: We support the recommendation of one stakeholder that where a person is charged for a cybercrime offence and/or where he or she is convicted, the fingerprints of the person should be taken and stored by the Criminal Records Office in accordance with the *Finger Prints Act.* Your Committee therefore recommends that the Ministry with responsibility for the *Finger Prints Act* urgently consider amending the Second Schedule of that legislation to include all offences under the *Cybercrimes Act.*

15. *Cybercrimes Act/Law Reform (Fraudulent Transactions)(Special Provisions) Act*: Your Committee noted the recommendation that the *Law Reform (Fraudulent Transactions)(Special Provisions) Act* and the Act be amended simultaneously, and the comment that a criminal action could be an offence under both Acts. **We suggest that the Ministry with responsibility for the *Law Reform (Fraudulent Transactions)(Special Provisions) Act* engage the process for the review of same.**

16. *The Sexual Offences Act*: It was recommended by one stakeholder that section 8 of the *Sexual Offences Act* be amended or the Act be revised to include a provision that was akin to section 63 of the Ghanaian Cybersecurity Act, 2020, which provides for dealing with child for purposes of sexual abuse. We do not support this recommendation as we were advised that section 4 of the Act already addresses the concern and that the proposals of the Joint Select Committee that reviewed of the *Sexual Offences Act* along with *the Offences Against the Person Act, the Domestic Violence Act and the Child Care and Protection Act* in its report seemed to be closely related. **We recommend that the relevant Ministries have consultation on the proposed provision.**

17. Aiding and abetting, and abetting of child dealing for the purposes of sexual abuse: One stakeholder recommended that section 9 of the *Sexual Offences Act* be amended to include the same level of specificity as section 64 of Ghana's Cybersecurity Act, 2020, which provides that *an owner or operator of a computer online service weblog internet service or internet bulletin board service shall not aid and abet another person for the purpose of facilitating or encouraging the online solicitation of a child, or permit any person to use the service of that person for the purpose of facilitating, encouraging, offering or soliciting unlawful sexual conduct of or with a child or the visual depiction of such conduct.* **We support the advice provided by the LRD that the MOEY consult the MOJ regarding enlarging the offence in section 9 of the *Sexual Offences Act*.** Additionally, it was pointed out by the LRD that based on the elements of the offence in section 64 of Ghana's legislation, it was realized that there had been a trend internationally toward regulating online content providers and internet service providers so that they play a more proactive role in monitoring contents uploaded on their systems and providing opportunities to have persons remove the contents where they have been uploaded. It was pointed out that the Joint Select Committee that reviewed the *Sexual Offences Act* along with *the Offences Against the Person Act, the Domestic Violence Act and the Child Care and Protection Act* in considering section 9 *Sexual Offences Act* recommended an adequate safeguard in terms of broadening the means of communication with children and broadening the scope of the offence to include persons. **The LRD further advised that if it were accepted that Jamaica should move towards regulating online service providers and social media, there would need to be discussion with the MOJ along with the MSET since the *Telecommunications Act* might be impacted. We support this advice.**

18. Skimmers/card readers: One entity that made a presentation to your Committee suggested that the possession of skimmers and card readers without lawful excuse should be an offence. We were informed by the MSET that the *Customs (Import Prohibition)(Miscellaneous Goods)(No. 2) Order, 2010,* specifies the different types of paraphernalia that could not be imported without meeting the conditions that were stipulated. Members of your Committee were advised that credit card scanning equipment could not be imported in Jamaica unless there was an import licence or permit, or prior approval was sought from the Minister with responsibility for national security. We noted that unlawful possession of credit cards/skimmers would be an offence in the redrafted section 10 of the Act, and if other paraphernalia such as magnetic strips and point-of-sale devices were to be considered, **it was recommended that the Ministry with responsibility for the *Customs Act* have the Order expanded to include the additional items. We support this recommendation.**

19. Intentionally withholding message delivered erroneously: Members of your Committee were informed by the MNS that victims were frequently subject to scams and fraud schemes, and have made genuine mistakes in sending messages as well as making payments to unintended recipients. We were advised that the Act currently does not allow for the prosecution of offenders who deliberately refused to cooperate in such instances, which would leave a victim to

pursue a civil lawsuit. It was noted that section 61 of the *Data Protection Act, 2020,* makes provision for personal data sent in error, and if the unintended recipients of the data actually used same to procure an advantage for himself or herself, the person would be liable for fraud under section 8 of the Act. **In respect of erroneous payment, your Committee recommends that the MNS recommends to the MOJ after consultation with stakeholders such as financial institutions, a possible amendment to the *Larceny Act* to create an offence similar to the Theft Act, 1968 of the United Kingdom which addresses the issue of dishonestly retaining a wrongful credit, and the inclusion of a provision to address payments made in error.**

20. Educational programme: Your Committee supports the proposal made that governmental entities such as the ODPP, the Jamaica Constabulary Force, the Financial Investigations Division and all investigating agencies such as the Jamaica Defence Force Military Intelligence take a joint approach to have an effective educational programme to allow them to be versed on the provisions of the Act in order to detect, investigate and prosecute offences under the Act.

21. Cybersecurity legislation: We noted during our deliberations that some of the general concerns raised by stakeholders would best be addressed in cybersecurity legislation such as the protection of critical systems, standards and guidelines for assessors of cyber services of protected systems, and the establishment of a cybersecurity authority. It was noted by one stakeholder that there should be guidelines and standards for the protection of protected computers; organisations with protected computers should be certified against standards; and vendors offering security services to entities with protected computers should be licensed. We were informed that the National Cyber Security Strategy, 2015, recognises the need for the establishment of standards and guidelines; the development of a national cybersecurity directorate; the development and adoption of cybersecurity technical guides for micro, small and medium enterprises; the strengthening of incident reporting and response; and the strengthening of partnership and cooperation. Members were advised that the *Information and Communications Technology Authority Act, 2019,* establishes and authorises a statutory body with responsibility for guiding the ICT affairs of public entities as well as recognizes the need for the ICT Authority to establish standards and guidelines that public entities were required to adhere to in relation to their IT systems and security. Additionally, the *Data Protection Act, 2020,* recognises the need for the establishment of standards and guidelines. **Notwithstanding these provisions, we are of the view that cybersecurity legislation may be necessary for protected computers in the private sector to conform to minimum standards and guidelines certification, and the licensing of vendors offering security services to private entities. However, the promulgation of cybersecurity legislation would require consultation with stakeholders and Cabinet's approval. We recommend that consideration be given to same.**

22. Responsible disclosure: Whilst one stakeholder suggested that a vulnerability disclosure framework be developed to allow individuals to report potential vulnerabilities without the threat of legal action, we were advised that JaCIRT facilitates the reporting of issues through its

website and the report could be anonymised. It was explained to us that there would be no threat of legal action and where vulnerability was verified, contact would be made to the owner of the IT resource and a joint effort would be made in respect of mitigation and/or remediation. **One Member of your Committee suggests that work be done to promote the present framework that operates through JaCIRT whilst fast tracking a more formalized framework in accordance to the European Union or other best practices across the world to ensure an open framework that applies to the public and private sectors.**

23. Protection of wireless network: It was recommended that wireless networks should be protected by mandating that they be password protected as a mitigating measure against cybercrime activities. Your Committee learned that the policy objective of the Government was to ensure access of the populace to the internet. **We support the recommendation that cybersecurity and data protection issues that may arise as a result of accessing public WI-FI be addressed in public education campaigns. We also support the view that entities that provide access to open WI-FI be encouraged to establish privacy and security statements relating to the use of their service.**

24. Legislative sandbox: It was recommended to your Committee that consideration be given to the granting of exemptions and open license in the context of academic freedom to conduct cross border exchange regarding teaching and research through the creation of a sandbox. JaCIRT defined a regulatory sandbox as *a contained environment in which regulated entities may test their products, services or solutions subject to the requirements under the subject framework.* We were informed of the two types of sandboxes, that is regulatory and industry sandboxes, which were developed by regulators and businesses respectively. We took note of the FinTech sandbox in Jamaica which was operated by the Bank of Jamaica (BOJ) and came about as part of the *Payment, Clearing and Settlement Act, 2010.*

JaCIRT pointed out to your Committee that the establishment of a sandbox would best be treated through policies within a sector rather than a generalized government approach and a framework being written into law. We were advised that whilst sandboxes provided the scope for innovation and testing of products at the pre-production and production levels before release, there was no supporting evidence through the research conducted where there was a generalised sandbox written into law. **We are of the view that a generalised sandbox could be explored in the near future given that the country currently did not have a regulatory framework for its creation or an entity designated as a regulator.**

5. ACKNOWLEDGEMENTS

Your Committee wishes to express its gratitude to the entities that made oral and written contributions on the Act. Special thanks are also extended to the technical team from the MSET; the OPC; the AGC; and the LRD.

Your Committee wishes to express thanks to the media, which ably reported on the proceedings of the meetings. Your Committee also wishes to thank the Clerk and the staff of the Houses of Parliament for their support and courtesies extended during the meetings.

Houses of Parliament
April, 2023

APPENDIX II
ATTENDANCE
TWENTY-ONE MEETINGS

Member	Present	Absent	Apologies
Hon. Daryl Vaz – **Chairman**	**19**	**2**	**2**
Hon. Floyd Green	**10**	**11**	**1**
Hon. Alando Terrelonge	**4**	**17**	**-**
Hon. Robert Nesta Morgan	**4**	**17**	**3**
Hon. Franklin Witter	**6**	**15**	**-**
Ms Tamika Davis	**10**	**11**	**1**
Ms Kerensia Morrison	**10**	**11**	**-**
Mr Julian Robinson	**18**	**3**	**3**
Mr Hugh Graham	**1**	**20**	**1**
Senator the Hon. Matthew Samuda	**12**	**9**	**3**
Senator Kavan Gayle	**21**	**-**	**-**
Senator Dr. Saphire Longmore	**21**	**-**	**-**
Senator Natalie Campbell Rodriques	**20**	**1**	**1**
Senator Peter Bunting	**13**	**8**	**3**
Senator Gabriela Morris	**17**	**4**	**-**
*Senator Sherene Golding Campbell	**10**	**-**	**-**

***Member could only have attended a maximum of ten (10) meetings.**

SIGNATURES

Hon. Daryl Vaz – **Chairman** .....

Hon. Floyd Green .....

Hon. Alando Terrelonge .....

Hon. Robert Nesta Morgan .....

Hon. Franklin Witter .....

Ms Tamika Davis .....

Ms Kerensia Morrison .....

Mr Julian Robinson .....

Mr Hugh Graham .....

Senator the Hon. Matthew Samuda .....

Senator Kavan Gayle .....

Senator Dr. Saphire Longmore .....

Senator Natalie Campbell Rodriques .....

Senator Peter Bunting .....

Senator Gabriela Morris .....

Senator Sherene Golding Campbell .....