Trinidad & Tobago Computer Society

112A Edward Street, Port of Spain,
Trinidad and Tobago
Website: http://ttcs.tt/ ; Email: info@ttcs.tt

June 16 2017

The Secretary
The Joint Select Committee on the Cybercrime Bill, 2017
Office of the Parliament of Trinidad and Tobago
Level 3, Tower D
International Waterfront Centre
1A Wrightson Road
Port-of-Spain

Re : TTCS Comments on the Cybercrime Bill 2017

Dear Secretary,

The Trinidad and Tobago Computer Society (TTCS ; http://ttcs.tt/) welcomes the opportunity to provide comments on the Cybercrime Bill 2017. Overall, we feel that the bill is generally well crafted and and deals with many issues that Trinidad and Tobago will encounter in the future. However, there are few areas of concern that we would like to share. These are;

1. Suppression of free speech and the work of journalists
   It is important to note that many of the clauses in this Bill can be applied to journalists carrying out their duties, and/or the free speech of private citizens, as well as to persons who are attempting, in the public interest, to report misconduct (aka whistleblowers). In the interest of support of the Fourth Estate as well as the principles of Free Speech enshrined in our Constitution, this Bill requires urgent complementary whistleblower/journalist protection via legislation.

2. Excessive Penalties
   A number of sections outline penalties of $100,000 to $3,000,000. These are non-trivial amounts that far exceed the penalties in other areas that many would view as more serious - for example drunk driving. We wonder if the concept of proportionality could be incorporated in this act.
   The quantum of penalties will have chilling effect on the legitimate use of computers and networks, for example, students learning about computer security and security professionals investigating vulnerabilities on behalf of their clients.

3. Collateral Damage
   The general trend in technology has been to move towards using shared server resources in the cloud. This opens up the possibility that data and equipment in use by accused persons may be simultaneously used by other persons unrelated to the accused and may thus be unduly affected by the shutdown and/or seizure of such equipment and data. Care must be taken to protect those who are not party to the criminal activities of other persons.

4. Potential for Censorship and Abuse
   In the interest of protecting the rights of citizens, we believe that all requests for access systems and data should be approved by the Judiciary via the application for, and receipt of, a warrant. This judicial warrant would ensure that any potential for abuse by the State, or its agents, would be mitigated.

5. Self Incrimination
   Several sections of this Bill seem to run afoul of the Constitution's directive that persons are protected from self incrimination, for example, the requirement that persons unlock their phones or decrypt their data in furtherance of an investigation. This is a dangerous issue and should be reconsidered.

6. Training.
   It is highly likely that the Courts and Trinidad and Tobago Police Service will be called on to deal many cases under this legislation. As such, it is critical that officers of both agencies receive training in some of technical issues surrounding cyber crime. In this regard the TTCS would welcome the opportunity to assist in providing this training and any specialized advice when required.

More detailed comments and observations relating to specific clauses are included below and on the online document at www.ttcs.tt/cybercrime2017-comments where you can find a history of the comments and discussions by TTCS members. If you have any questions, please do not hesitate to contact us at info@ttcs.tt . Thank you again for the opportunity to submit our comments and concerns.

Yours Faithfully,

Dev Anand Teelucksingh
Secretary

PART I - PRELIMINARY

			TTCS comments / observations
Short title	1.	This Act may be cited as the Cybercrime Act, 2017	An observation that some sections are similar to Saint Vincent and the Grenadines Cybercrime Bill http://www.assembly.gov.vc/assembly/images/stories/cybercrime%20bill%202016.pdf
Commencement	2.	This Act comes into operation on such date as is fixed by the President by Proclamation.	
Act inconsistent with Constitution	3.	3. This Act shall have effect even though inconsistent with sections 4 and 5 of the Constitution.	To be determined? http://rgd.legalaffairs.gov.tt/laws2/Constitution.pdf 4. Recognition and declaration of rights and freedoms. 5. Protection of rights and freedoms.
Interpretation	4.	In this Act – "computer data" means any representation of – (a) facts; (b) concepts; (c) machine-readable code or instructions; or (d) information, including text, sound, 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 includes a program that can cause a computer system to perform a function; "computer data storage medium" means anything in which information is capable of being stored, or anything from which information is capable of being retrieved or reproduced, with or without the aid of any other article or device;	

		"computer program" or "program" means 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 program or external instruction to perform automatic processing of information or electronic data; "data message" has the meaning assigned to it in the Electronic Transactions Act; "device" means any electronic programmable device used, whether by itself or as part of a computer network, an electronic communications network or any other device or equipment, or any part thereof, to perform pre-determined arithmetic, logical, routing or storage operations and includes – (a) an input device; (b) an output device; (c) a processing device; (d) a computer data storage medium; (e) a program; or (f) equipment, that is related to, connected with or used with such a device or any part thereof; "electronic mail message" means an unsolicited data message, including electronic mail and an instant message; "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; "hinder" in relation to a computer system, 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) inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data; "internet service provider" includes a person who provides the services referred to in Part IV; "Minister" means the minister to whom responsibility for national security is assigned; "remote forensic tools" means investigative software or hardware installed on or attached to a computer system that is used to perform a task that includes keystroke logging or transmission of an internet protocol address; "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 the chain of communication; and (c) shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services, and references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other.	

PART II - CYBERCRIME OFFENCES

Illegal access to a computer system	5.	A person who, intentionally and without lawful excuse or justification, accesses a computer system or any part of a computer system, commits an offence and is liable – (a) on summary conviction to a fine of three hundred thousand dollars and imprisonment for three years; or	Just an observation that this clause would allow for someone accessing an unsecured Wifi to be charged. Why are these fines so high? According http://www.trinidadexpress.com/news/Biggers-fines-for-drunk-drivers-street-racers-291075441.html , Motorists who drive drunk will now have to pay fines ranging from

		(b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for five years.	$12,000 to $22,500. Online fines should bear some resemblance to their nearest offline equivalence.
Illegally remaining in a computer system	6.	A person who, intentionally and without lawful excuse or justification, remains logged into a computer system or part of a computer system or continues to use a computer system commits an offence and is liable – (a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or (b) on conviction on indictment to a fine of two hundred thousand dollars and imprisonment for three years.	
Illegal data interference	7.	(1) A person who, intentionally and without lawful excuse or justification – (a) damages computer data or causes computer data to deteriorate; (b) deletes computer data; (c) alters computer data; (d) copies computer data to any computer data storage device or to a different location within the computer system; (e) moves computer data to a computer storage device or a different location within the computer system; (f) renders computer data meaningless, useless or ineffective; (g) obstructs, interrupts or interferes with the lawful use of computer data; (h) obstructs, interrupts or interferes with a person in his lawful use of computer data; or (i) denies access to computer data to a person who is authorised to access it, commits an offence.	Illegal data interference which is more damaging than clause 5 (“Illegal access to a computer system”) attracts lower penalties than 5? What is the outcome if someone denies access to a computer which affects 1000 people? Is this fine multiplied by 1000? Need clarification. This might be critical for infrastructure things like SCADA systems, which have the potential to affect tens of thousands, at minimum. Maybe different classes of offense? There seems to be significant overlap with earlier clauses.

		(2) A person who commits an offence under subsection (1), is liable – (a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or (b) on conviction on indictment to a fine of two hundred thousand dollars and imprisonment for three years.	
Illegal acquisition of data	8.	(1) A person who intentionally and without lawful excuse or justification accesses a computer system without authorisation, or by exceeding authorised access, and obtains computer data commits an offence and is liable – (a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for three years. (2) A person who intentionally and without lawful excuse or justification receives or gains access to computer data knowing the same to have been stolen or obtained pursuant to sub-section (1) commits an offence and is liable – (a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for three years.	The clause will likely get whistleblowers and/or press in trouble with such disclosure. Because part 2 seems to say that any press receiving the data is guilty of a crime. There needs some form of protection for whistleblowers and journalists and news media.
Illegal system interference	9.	(1) A person who, intentionally and without lawful excuse or justification, hinders or interferes with a computer system commits an offence (2) A person who, intentionally and without lawful excuse or justification, hinders or interferes with a person who is lawfully using or operating a computer system commits an offence. (3) A person who commits an offence under this section is liable – (a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; or (b) on conviction on indictment to a fine of three hundred thousand dollars dollars and imprisonment for three years.	Would investigating officers and courts be sophisticated enough to understand the nuances of these issues? For example, most malware spreads from compromised machines unaware by the owner of compromised machines .

Offences affecting critical infrastructure	10.	(1) Notwithstanding the penalties set out in sections 5 to 9, where a person commits an offence under any of those sections and the offence results in hindering, or interference with, a computer system that – (a) is exclusively for the use of critical infrastructure; or (b) affects the use, or impacts the operation, of critical infrastructure, he is liable on conviction on indictment to a fine of two million dollars and imprisonment for fifteen years. (2) For the purpose of this section, "critical infrastructure" means any computer system, device, network, computer program or computer data so vital to the State that the incapacity or destruction of, or interference with, such system, device, network, program or data would have a debilitating impact on the – (a) security, defence or international relations of the State; or (b) provision of services directly related to national or economic security, banking and financial services, public utilities, the energy sector, communications infrastructure, public transportation, public health and safety, or public key infrastructure.	Shouldn't the definition of critical infrastructure in 10 (2) be in the definitions under part 1 #4 ? Maybe system critical financial services to distinguish between a large bank or insurance company vs. small money changers.
Illegal devices	11	(1) A person who – (a) produces, sells, procures for use, imports, exports, distributes or otherwise makes available or has in his possession – (i) a device, or computer program, that is designed or adapted for the purpose of committing an offence under this Act; or (ii) a computer password, access code or similar data by which the whole or any part of a computer system, computer data storage device or computer data is capable of being accessed, with the intent that it be used for the purpose of committing an offence under this Act; or (b) intentionally and without lawful excuse or justification discloses a computer password, access code or similar data by which the whole or any part of a computer system, computer data storage device or computer data can be accessed -	If this were to criminalise the use of security tools (eg. Wireshark)? This is problematic for the entire field of penetration testing and computer forensics. However the last phrase in 11 a (ii) seems to look at the intent behind of the use of these programs. So a network admin using pen testing tools is fine but a hacker using the same tools to break into an organization has committed an offence. The language needs to accommodate legitimate users who are engaged in securing computer networks. 11 (1) (b) seems to be misplaced here under a heading of "illegal devices" and perhaps could be deleted or merged

		(i) for unlawful gain, whether for himself or another person; (ii) for an unlawful purpose; or (iii) knowing that it is likely to cause unlawful damage, commits an offence. (2) A person who commits an offence under subsection (1) is liable – (a) on summary conviction to a fine of two hundred thousand dollars and imprisonment for three years; or (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for five years.	with 12.
Unauthorised granting of access to computer data	12	(1) A person who, through authorised or unauthorised means, obtains or accesses computer 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 unauthorized access, and intentionally and without lawful excuse or justification grants access to or gives the computer data to another person, whether or not he knows that the other person is authorised to receive or have access to the computer data, commits an offence. 2) A person who commits an offence under this section is liable – (a) on summary conviction to a fine of two hundred thousand dollars and imprisonment for three years; and (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for five years.	Need clear definition on matters of ”national security” The latter clause regarding justification (“lawful excuse”) though may be the intended link to possible whistleblower legislation which is needed. As stated before, there needs to be to be some form of protection for whistleblowers, journalists, and news media.
Computer-related forgery	13	(1) A person who, intentionally and without lawful excuse or justification inputs, alters, deletes or suppresses computer data, resulting in inauthentic data, with the intent that it be considered or acted upon 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 hundred thousand dollars and imprisonment for three years; or	Just noticed that point (2) of this computer forgery has nothing to do with forgery. It speaks about email spamming and may need to be place at another area in the document.

		(b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for five years. (2) A person who commits an offence under subsection (1) by sending out multiple electronic mail messages from or through a computer system, is liable on conviction to a fine of two hundred thousand dollars and imprisonment for three years, in addition to the penalty set out in subsection (1).	
Computer-related fraud	14	(1) A person who, intentionally and without lawful excuse or justification – (a) inputs, alters, deletes or suppresses computer data; or (b) interferes with the functioning of a computer system, with the intent of procuring an economic benefit for himself or another person and thereby causes loss of, or damage to, property, commits an offence. (2) A person who commits an offence under subsection (1) is liable – (a) on summary conviction to a fine of one million dollars and imprisonment for five years; or (b) on conviction on indictment to a fine of two million dollars and imprisonment for ten years.	Just an observation that this would target ransomware like the recent Wannacry (https://en.wikipedia.org/wiki/WannaCry_ransomware_attack) This doesn't appear to cover other types of malware (https://en.wikipedia.org/wiki/Malware) such as viruses but this appears to be covered under clause 9
Identity-related offences	15	A person who intentionally transfers, possesses or uses a means of identification, other than his own, with the intent of committing an unlawful act through the use of a computer system, commits an offence and is liable – (a) on summary conviction to a fine of three hundred thousand dollars and imprisonment for three years; or (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for five years.	
Violation of privacy	16.	(1) A person who intentionally and without lawful excuse or justification – (a) captures; or (b) stores in, or publishes or transmits through a computer system,	Would the images of private areas of a person also apply if persons were in undergarments when images were taken?

		the image of the private area of another person without his consent, where the other person has a reasonable expectation that he could disrobe in privacy, or that his private area would not be visible to the public regardless of whether he is in a public or private place, commits an offence. (2) A person who commits an offence under subsection (1) is liable – (a) on summary conviction to a fine of one hundred thousand dollars and imprisonment for two years; and (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for three years. (3) For the purposes of this section, “private area” means the genitals, pubic area, buttocks or breast.	
Causing damage by electronic mail message	17	(1) A person who maliciously initiates, relays or re-transmits an electronic mail message from or through a computer system and thereby causes damage to a computer system commits an offence. (2) A person who intentionally falsifies the header information of an electronic mail message for the purpose of committing an offence under subsection (1) commits an offence. (3) A person who commits an offence under this section is liable – (a) on summary conviction to a fine of three hundred thousand dollars and imprisonment for three years; and (b) on conviction on indictment to a fine of five hundred thousand dollars and imprisonment for five years.	Just curious about how intent is proven. Email worms that spread themselves or users who unknowingly forward these messages could be a tricky issue.
Causing harm by communication using a computer system	18	(1) A person who uses a computer system to communicate with the intention to cause harm to another person commits an offence.	This area is problematic. Clauses like this have already been used in other Caribbean countries to suppress free speech by activists. Any comment criticizing a public figure could be construed as causing serious emotional

		(2) In determining whether an offence is committed under this section, the Court may take into account any factor which it considers relevant, including – (a) the extremity of the language used in the communication; (b) the age and characteristics of the person involved; (c) whether the communication was anonymous; (d) whether the communication was repeated; (e) the extent of circulation of the communication; (f) whether the communication is true or false; and (g) the context in which the communication appeared. (3) A person who commits an offence under this section is liable – (a) on summary conviction to a fine of one hundred thousand dollars and to imprisonment for three years; and (b) on conviction on indictment to a fine of two hundred and fifty thousand dollars and imprisonment for five years. (4) For the purposes of this section, “harm” means serious emotional distress.	distress. The concept of a public figure should change the level of activity that constitutes “causing harm”. Public figures should and do, expect a certain amount of comment on their public activities. This is not the case for private citizens. The bar for “harm” should be set much higher for public figures. “Serious emotional distress” is not the only repercussion that may arise - for example, doxxing, or the release of personal information, such as phone numbers and addresses, can lead to actual physical harm. Perhaps to cover this, Part 4 “harm” should be changed to “For the purposes of this section, “harm” **includes** serious emotional distress.” Reputational damage is already covered by existing law.
Intent to extort a benefit	19	A person who uses a computer system with the intent to extort a benefit from another person by threatening to publish computer data containing personal or private information which can cause public ridicule, contempt, hatred or embarrassment commits an offence and is liable – (a) on summary conviction to a fine of one hundred thousand dollars and to imprisonment for three years; and (b) on conviction on indictment to a fine of two hundred and fifty thousand dollars and imprisonment for five years.	

PART III - ENFORCEMENT

Jurisdiction	20	(1) A Court in Trinidad and Tobago 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 Trinidad and Tobago; (b) by a citizen of Trinidad and Tobago, whether in Trinidad and Tobago or elsewhere; or (c) by a person on board a vessel or aircraft registered in Trinidad and Tobago. (2) For the purpose of subsection (1)(a), an act is carried out in Trinidad and Tobago if – (a) the person is in Trinidad and Tobago at the time when the act is committed; (b) a computer system located in Trinidad and Tobago or computer data on a computer data storage device located in Trinidad and Tobago is affected by the act; or (c) the effect of the act, or the damage resulting from the act, occurs within Trinidad and Tobago. (3) Subject to subsection (1), a Summary 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 program or computer data which the accused used, was within the magisterial district at the time when he committed the offence; or (c) damage occurred within the magisterial district, whether or not paragraph (a) or (b) applies.	This does seem to clear the way for charging someone whose data is hosted on outside cloud services (Facebook, Twitter, web hosting companies) given the phrasing of “offence is carried out wholly or partly in Trinidad and Tobago” if the effect of the act or the damage resulting from the act, occurs within Trinidad and Tobago.
Search and seizure	21	(1) Where a Magistrate is satisfied on the basis of information on oath by a police officer that there is reasonable ground to believe that there is in a place an apparatus or computer data – (a) that may be material as evidence in proving an offence under this Act; or	Police officers and court officers need to be trained and educated on the implications of this clause. If the place where an apparatus or computer data that may be material as evidence in proving an offence is a third party hosting center or business place, the seizing of apparatus or

		(b) that has been acquired by a person as a result of an offence under this Act, he may issue a warrant authorizing a police officer, with such assistance as may be necessary, to enter the place to search for and seize the apparatus or computer data. (2) If a police officer who is undertaking a search under this section has reasonable grounds to believe that – (a) the computer data sought is stored in another apparatus; or (b) part of the computer data sought is in another place within Trinidad and Tobago, and such computer data is lawfully accessible from, or available to the first apparatus, he may extend the search and seizure to that other apparatus 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 computer data storage media; (b) make and retain a copy of computer data; (c) remove computer data in a computer system or render it inaccessible; (d) take a printout of the output of computer data; (e) impound or similarly secure a computer system or part of it or a computer data storage medium; or (f) remove a computer system or computer data storage medium from its location. (4) A police officer who undertakes a search under this section shall secure any apparatus and maintain the integrity of any computer data that is seized. (5) For the purpose of this section, “apparatus” includes – (a) a computer system or part of a computer system; or (b) a computer data storage medium.	computer data under clause 3(c) (“ remove computer data in a computer system or render it inaccessible;”) could collect data from other users not in the warrant and also severely disrupt the business operations of such a company and other users of the said apparatus.
Assistance	22	(1) A person who has knowledge about the functioning of an apparatus, or measures applied to protect computer data, that	We note that this clause would allow for encrypted data to be decrypted or person’s mobile phones to be unlocked.

		is the subject of a search warrant shall, if requested by the police officer authorised to undertake the search, assist the officer by – (a) providing information that facilitates the undertaking of the search for and seizure of the apparatus or computer data sought; (b) accessing and using an apparatus to search computer data which is stored in, or lawfully accessible from, or available to, that apparatus; (c) obtaining and copying computer data; or (d) obtaining an intelligible output from an apparatus in such a format that is admissible for the purpose of legal proceedings. (2) A person who fails to comply with this section commits an offence and is liable on summary conviction to a fine of one hundred thousand dollars and imprisonment for one year.	When devices and data are decrypted or unlocked in this way, there's the risk of private legitimate communications with innocent third parties being exposed. Potentially if the data on the apparatus is provided by a third party (business, data center) is encrypted by a user, it cannot be expected for such a third party to be able to decrypt such information. It must be acknowledged that in certain instances, for example in the case of data encrypted by a third party or technical deficiency on the part of the person, it may not be reasonable or even possible for the person to be of assistance in producing the required data or access. In such cases, it would not be advisable for such a person to be unfairly prosecuted.
Order for removal or disablement of data	23	If a Magistrate is satisfied on the basis of information on oath by a police officer that an internet service provider or any other entity with a domain name server is storing, transmitting or providing access to information in contravention of this Act or any other written law, the Magistrate may order the internet service provider or other entity with a domain name server to remove, or disable access to, the information.	This clause is problematic to implement. According to the Internet Society's White Paper titled "Perspectives on Internet Content Blocking: An Overview" dated March 2017 at https://www.internetsociety.org/doc/internet-content-blocking : "The Internet Society believes the most appropriate way to counteract illegal content and activities on the Internet is to attack them at their source. Using filters to block access to online content is inefficient, likely to be ineffective, and is prone to generate collateral damage affecting innocent Internet users." The Internet Society report should be read in its entirety at https://www.internetsociety.org/doc/internet-content-blocking
Production Order	24	If a Magistrate is satisfied on the basis of information on oath by a police officer that computer data, a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, the Magistrate may order	Again, as mentioned in clause 22 comments, if the data on the apparatus provided by a third party (business, data center) is encrypted by a user, it cannot be expected for such a third party to be able to decrypt such

		– (a) a person in Trinidad and Tobago who is in control of an apparatus, to produce from the apparatus computer data or a printout or other intelligible output of the computer data; or (b) an internet service provider in Trinidad and Tobago to produce information about a person who subscribes to, or otherwise uses his service.	information. Forcing a person to unlock their device or decrypt their data can be considered a form of self-incrimination, which is inconsistent with the provisions of Section 5 of the Constitution: “Parliament may not...authorise a Court, tribunal, commission, board or other authority to compel a person to give evidence unless he is afforded protection against self-incrimination and, where necessary to ensure such protection, the right to legal representation” http://rgd.legalaffairs.gov.tt/laws2/Constitution.pdf
Expedited preservation	25	(1) A Magistrate may, if satisfied on an ex parte application by a police officer of the rank of Superintendent or above, that there are grounds to believe that computer data that is reasonably required for the purpose of a criminal investigation is vulnerable to loss or modification, authorise the police officer to require a person in control of the computer data, by notice in writing, to preserve the data for such period not exceeding ninety days as is stated in the notice. (2) A Magistrate may, on an ex parte application by a police officer of the rank of Superintendent or above, authorise an extension of the period referred to in subsection (1) by a further specified period not exceeding ninety days.	Especially in the case of multimedia data, storage and retrieval/transmission costs can be extremely expensive when stored overseas, especially for the length of time potentially required by this law. This can have a severe impact on a third party service or hosting provider, both on their ability to service the request for storage and their ability to continue running their business.
Disclosure of details of an order	26	(1) If an order under section 24 or a notice under section 25 stipulates that confidentiality is to be maintained, a person who is the subject of the order or notice and who intentionally and without lawful excuse or justification discloses – (a) the fact that the order or notice has been made; (b) the details of the order or notice; (c) anything done pursuant to the order or notice; or (d) any data collected or recorded pursuant to the order, commits an offence. (2) A person who commits an offence under subsection (1) is liable –	It is not clear whether the person subject to the order is able to challenge the order in the courts in cases where the requirements of clauses 24 and 25 are unreasonably onerous or potentially damaging to their business. It is also unclear in this and other clauses in the bill as to what happens to data collected in investigations are no longer needed or relevant by authorities. The data collected must be properly secured for the duration of the investigation and properly destroyed or returned to the persons subject to the order.

		(a) on summary conviction to a fine of one million dollars and imprisonment for three years; or (b) on conviction on indictment to a fine of two million dollars and imprisonment for five years.	Information collected by authorities can include sensitive data from unrelated third parties and care must be taken to protect their privacy.
Disclosure of traffic data	27	If a Magistrate is satisfied on the basis of information on oath by a police officer, that there are reasonable grounds to believe that computer data stored in an apparatus is reasonably required for the purpose of a criminal investigation into a data message, he may require a person to disclose sufficient traffic data about the data message to identify – (a) the internet service provider; or (b) the path, through which the data message was transmitted.	It may not be technically feasible to accurately determine the entire path through which the data has passed; for example, extensive logs may not have been kept. ISPs should therefore not prosecuted for an inability to comply.
Remote forensic tools	28	(1) If a Judge is satisfied on ex parte application by a police officer, that there are reasonable grounds to believe that computer data which is required for the purpose of a criminal investigation into an offence listed in the Schedule 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 such 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, and the extent and duration of its utilization; and (d) reason for the use of the tool. (3) Where an application is made under subsection (1), the Judge may order that an internet service provider support the installation of the remote forensic tool. (4) Where a remote forensic tool is utilised under this section –	This clause appears to contradict the Interception of Communications Act 2010. This clause should therefore be adjusted in consideration of the powers already conferred to authorities under this act. Also, there may be a risk that a police officer can plant false evidence through the use of a remote forensic tool. Potentially, a remote forensic tool could be subverted by hackers and compromise the suspect's data and potentially other unrelated computers connected to the suspect's computer. There may be an issue of jurisdiction. Suppose the computer data is located outside of Trinidad and Tobago, can this clause allow for local courts to authorize use of remote forensic tools in computers outside of Trinidad and Tobago?

		(a) modifications to a computer system shall be limited to those that are necessary for the investigation; (b) modifications to a computer system shall be undone, so far as possible, after the investigation; and (c) the following information shall be logged: (i) the technical means 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 authorization that is granted under this section 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 authorization are no longer present. (7) The Minister may, by Order, amend the Schedule. (8) For the purpose of this section, “utilise” includes – (a) accessing a computer system; (b) developing a remote forensic tool; (c) adopting a remote forensic tool; or (d) acquiring a remote forensic tool.	
Order for payment of additional fine	29	(1) Where a person is convicted of an offence under this Act and the Court is satisfied that monetary benefits accrued to him as a result of the commission of the offence, the Court may order him to pay an additional fine in an amount equal to the amount of the monetary benefits. (2) Where damage is caused as a result of an offence under this	

		Act, the person convicted of the offence is liable to an additional fine not exceeding the fine that the Court may impose for the commission of the offence that caused the damage.	
Order for payment of compensation	30	(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, it 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 or likely to be 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 damage may have under any other law. (3) The Court may make an order under this section of its own motion or upon application of a person who has suffered damage as a result of the commission of the offence. (4) A person who makes an application under subsection (3) shall do so before sentence is passed on the person against whom the order is sought. (5) For the purpose of this section, computer data held in an apparatus is deemed to be the property of the owner of the apparatus.	Part 5 regarding who is the owner of the computer data held in an apparatus is deemed to be the property of the owner of the apparatus does not seem to take into account cloud storage practices or outsourcing of data storage where the owner of the data is not necessarily the owner of the device on which it is stored.
Forfeiture Order	31	(1) Subject to subsection (2), where a person is convicted of an offence under this Act, the Court may 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 claims to be the owner of the property or who appears to the Court to have an interest in the property. (3) Property forfeited to the State under subsection (1) shall vest in the State— (a) if no appeal is made against the order, at the end of the period within which an appeal may be made against the order;	Subsection 4 should take into account the possibility that sensitive data pertaining to third-parties may be exposed and care must be taken to protect or properly destroy such data and equipment.

		or (b) if an appeal has been made against the order, on the final determination of the matter, where the decision is made in favour of the State. (4) Where property is forfeited to the State under this section, it shall be disposed of in the prescribed manner.	
Order for seizure and restraint	32	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 31 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 that property if found, and any other property in respect of which the police officer believes, on reasonable grounds, that a forfeiture order under section 31 may be 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.	

Part IV - Internet Service Providers

No monitoring obligation	33	(1) Subject to subsection (2), an internet service provider who provides a conduit for the transmission of information, shall not be responsible for – (a) monitoring the information which he transmits or stores on behalf of another in order to ascertain whether its processing would constitute or give rise to liability under this Act; or (b) actively seeking facts or circumstances indicating illegal activity in order to avoid criminal liability under this Act. (2) Subsection (1) does not relieve an internet service provider from complying with any court order, injunction, writ or other	

		legal requirement, which obliges an internet service provider to terminate or prevent an infringement based on any written law.	
Access provider	34	(1) An access provider shall not be liable under this Act for providing access and transmitting information if he does not – (a) initiate the transmission; (b) select the receiver of the transmission; or (c) select or modify the information contained in the transmission. (2) For the purpose of this section – “access provider” means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by transmitting information provided by, or to a user of the service in a communication network or provides access to a communication network; “communication network” means a set of devices or nodes connected by communication links, which is used to provide the transfer of computer data between users located at various points or other similar services; and “transmit” or “provide access” includes the automatic, intermediate and transient storage of information transmitted in so far as it takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for a period longer than is reasonably necessary for the transmission.	
Hosting provider	35	(1) A hosting provider shall not be liable for the storage of information in contravention of this Act if – (a) he expeditiously removes or disables access to the information after receiving a lawful order from any appropriate authority to remove specific illegal information stored; or (b) upon obtaining knowledge or awareness, by ways other than a lawful order from any appropriate authority, about specific illegal information stored, he expeditiously informs the authority to enable it to evaluate the nature of the information and, if necessary, issue an order to remove the	This may delay the ability of the Hosting Provider to protect their network.

		content. (2) This section shall not apply when the user of the service is acting under the authority or control of the hosting provider. (3) For the purpose of this section – “hosting provider” means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by storing information provided by a user of his service.	
Caching provider	36	(1) A caching provider shall not be liable for the storage of information in contravention of this Act if – (a) he does not modify the stored information; (b) he complies with the condition of access to the stored information; (c) he updates stored information in accordance with any written law or in a manner that is widely recognised and used in the information communication technology industry; or (d) he does not interfere with the lawful use of technology, widely recognised and used by the information communication technology industry, to obtain data on the use of the stored information, and acts expeditiously to remove or to disable access to the information he has stored upon obtaining knowledge of the fact that – (e) the stored information at the initial source of the transmission has been removed from the network; (f) access to the stored information has been disabled; or (g) a Court has ordered the removal or disablement of the stored information (2) For the purpose of this section – “caching provider” means a person who provides a service to facilitate the transmission of computer data between two or more computer systems by the automatic, intermediate and temporary storage of information, where such storage is for the sole purpose of making the onward transmission of the information to other users of the service more efficient.	

Hyperlink provider	37	(1) An internet service provider who enables the access to information provided by another person, by providing an electronic hyperlink, shall not be liable for information that is in contravention of this Act if – (a) the internet service provider expeditiously removes or disables access to the information after receiving a lawful order from any appropriate authority to remove the link; or (b) the internet service provider, upon obtaining knowledge or awareness, by ways other than a lawful order from any appropriate authority, expeditiously informs the authority to enable it to evaluate the nature of the information and if necessary issue an order to remove the content. (2) For the purpose of this section – “hyperlink” means a characteristic or property of an element such as a symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed.	As mentioned in clause 23, this clause is problematic to implement. According to the Internet Society’s White Paper titled “Perspectives on Internet Content Blocking: An Overview” dated March 2017 at https://www.internetsociety.org/doc/internet-content-blocking : “The Internet Society believes the most appropriate way to counteract illegal content and activities on the Internet is to attack them at their source. Using filters to block access to online content is inefficient, likely to be ineffective, and is prone to generate collateral damage affecting innocent Internet users.”
Search engine provider	38	A provider who makes or operates a search engine that either automatically, or based on entries by others, creates an index of internet-related content or, makes available electronic tools to search for information provided by another person, shall not be liable under this Act for the search results if the provider – (a) does not initiate the transmission; or (b) does not select the receiver of the transmission; or (c) does not select or modify the information contained in the transmission.	

Part V - Miscellaneous

Regulations	39	(1) 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. (2) Regulations made under this section shall be subject to negative resolution of Parliament.	
Review of the Act	40	The Minister shall cause the Act to be reviewed at least once every three years from the date on which it comes into operation.	Does this imply that the act expires if not renewed every three years?
Repeal of Chap. 11:17	41	The Computer Misuse Act is repealed.	

SCHEDULE - OFFENCES

	1	Offences involving treason under the Treason Act, Chap. 11:03	
	2	Offences against the person, namely – (a) Murder (b) Manslaughter	
	3	Offences involving kidnapping	
	4	Drug trafficking, namely – (a) Trafficking in dangerous drugs; (b) Possession of a dangerous drug for the purpose of trafficking	
	5	Unlawful possession of a firearm or ammunition	
	6	Offences involving a terrorist act	
	7	Trafficking in persons or trafficking in children	
	8	Offences involving child pornography	
	9	Offences involving fraud	
	10	Offences involving corruption	
	11	Offences involving money laundering	
	12	Offences affecting critical infrastructure	
	13	Tax offences	