PARLIAMENT
REPUBLIC OF TRINIDAD AND TOBAGO

Secretariat Unit

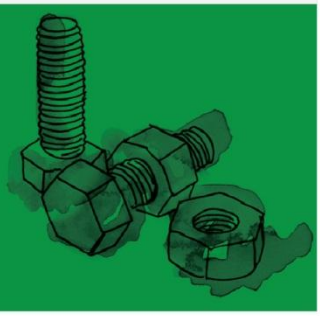
Bill Essentials

THE CYBERCRIME BILL, 2014

An Act to provide for the creation of offences related to cybercrime and related matters

Introduced in: The House of Representatives

Introduced on: 21 March,2014



BACKGROUND

The Bill was introduced in the House of Representatives on Friday March 21, 2014. It is based on Government's recognition of the importance of Information and Communication Technologies (ICTs) to the advancement of national development.[1] Cybercrime is a growing threat, which encompasses any criminal act relating to computers and computer networks.[2] Cognizant of the value and significance of electronic communications and the resultant opportunities that ICTs bring, and the associated risks in operating in such an environment, the Government saw the need to enact legislation that would provide for the creation of offences related to cybercrime and for other related matters.

RELATIVE LEGISLATION REFERRED TO IN THE BILL

- The Electronic Transactions Act, 2011[3];
- The Interception of Communications Act, 2010[4];
- The Community Service Orders Act[5]; and
- The Treason Act[6], Chap. 11:03.

[1] Government of Trinidad and Tobago National Cyber Security Strategy. 2012. Pgs. 1-4. http://www.nationalsecurity.gov.tt/Portals/0/Pdf%20Files/National_Cyber_Security%20Strategy_Final.pdf
[2] Webopedia. Cybercrime. http://www.webopedia.com/TERM/C/cyber_crime.html
[3] Electronic Transactions Act, 2011. http://www.ttparliament.org/legislations/a2011-06.pdf
[4] The Interception of Communications Act, 2010. https://www.ttbizlink.gov.tt/trade/tnt/cmn/pdf/Interceptions%20Act.pdf
[5] Community Service Orders Act. http://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/13.06.pdf
[6] Treason Act Chap. 11:03. http://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/11.03.pdf

KEY FEATURES OF THE PROPOSED LEGISLATION

Among other amendments, the Bill:

- ✓ makes provision for the Act to come into operation on proclamation by the President;

- ✓ makes provision for the Act to have effect though inconsistent with the Constitution;

- ✓ provides definitions for certain terms used in the Bill;

- ✓ makes it an offence to illegally access a computer system and would carry a fine of three hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment;

- ✓ makes it an offence to illegally remain logged in to a computer system and this would carry a fine of one hundred thousand dollars and two years' imprisonment on summary conviction or a fine of two hundred thousand dollars and three years' imprisonment on conviction on indictment;

- ✓ makes it an offence to illegally intercept non-public transmission or electromagnetic emissions to or from a computer system and would carry a fine of two hundred and fifty thousand dollars and imprisonment for three years on summary conviction or affine of five hundred thousand dollars and five years' imprisonment on conviction on indictment;

- ✓ makes it an offence to illegally interfere with computer data which would include damaging or deleting computer data. This offence would carry a fine of one hundred thousand dollars and two years' imprisonment on summary conviction or a fine of two hundred thousand dollars and three years' imprisonment on conviction on indictment;

- ✓ makes it an offence to illegally acquire computer data whether for personal use or for use by another person and would carry a fine of one hundred thousand dollars and two years' imprisonment on summary conviction or a

fine of five hundred thousand dollars and three years' imprisonment on conviction on indictment;

- ✓ makes it an offence to illegally interfere with a computer system or a person who is lawfully using or operating a computer system. This offence would carry a fine of one hundred thousand dollars and two years' imprisonment on summary conviction or a fine of three hundred thousand dollars and three years' imprisonment on conviction on indictment;

- ✓ also seeks to impose greater penalties on persons who commit an offence under Part II (Cybercrime Offences) of the Bill and which affects critical infrastructure which is defined as 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 security, defence or international relations of the State or the 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. Such an offence would carry a penalty of two million dollars and fifteen years imprisonment on conviction on indictment;

- ✓ makes it an offence to illegally produce, sell, procure, import, export, distribute or otherwise make available, a computer device or programme for the purpose of committing an offence under the Act. This offence would carry a fine of two hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment;

- ✓ makes it an offence for the unauthorized receipt or grant of access to computer data stored in a computer system and would carry a fine of two hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment;

- ✓ creates the offence of computer-related forgery which would make it unlawful to input, alter, delete or suppress computer data which would

result in inauthentic data. This offence would carry a fine of three hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment;

- ✓ creates the offence of computer related fraud which would carry a fine of one million dollars and five years' imprisonment on summary conviction or a fine of two million dollars and ten years' imprisonment on conviction on indictment;

- ✓ makes it an offence for identity theft through the use of a computer system and would carry a fine of three hundred thousand dollars and three years' imprisonment on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment;

- ✓ creates the offence of child pornography through the use of a computer system or other information and communication technology. This offence would carry a fine of one million dollars and ten years' imprisonment on summary conviction or a fine of two million dollars and fifteen years' imprisonment on conviction on indictment;

- ✓ creates the offence of luring, which is the use of a computer system to set up a meeting with a child for the purpose of abusing the child. This offence would carry a fine of one million dollars and ten years' imprisonment on summary conviction or a fine of two million dollars and fifteen years' imprisonment on conviction on indictment;

- ✓ makes it an offence to violate a person's privacy by capturing and sharing pictures or videos of a person's private area without his consent. Such an offence would carry a fine of one hundred thousand dollars and two years' imprisonment on summary conviction or a fine of five hundred thousand dollars and three years' imprisonment on conviction on indictment;

- ✓ seeks to criminalize the act of sending multiple electronic mail messages that are unsolicited and which causes harm to a person or damage to a computer. This offence would carry a fine of three hundred thousand dollars and three years' imprisonment on summary conviction or a fine of

five hundred thousand dollars and five years' imprisonment on conviction on indictment;

- ✓ makes it an offence to cause harassment through the use of electronic means with the intent to cause emotional distress. This offence would carry a fine of one hundred thousand dollars and three years' imprisonment on summary conviction or a fine of two hundred and fifty thousand dollars and five years' imprisonment on conviction on indictment;

- ✓ provides for the jurisdiction of the Courts of Trinidad and Tobago as it would relate to its territorial limits under the Act (where the offence is carried out wholly or partly in Trinidad and Tobago, by a citizen of Trinidad and Tobago whether in Trinidad and Tobago or elsewhere, or by a person on board a vessel or aircraft registered in Trinidad and Tobago);

- ✓ would impose liabilities for offences committed by a body corporate or any person purporting to act in such a capacity;

- ✓ would empower the Court to authorize the search and seizure of apparatus and computer data necessary for establishing an offence or which has been acquired by a person as a result of the commission of an offence;

- ✓ would impose liability on a person who has knowledge about the functioning of a computer system but who fails to render assistance to access computer data that is the subject of a search warrant;

- ✓ would empower a Magistrate to order an internet service provider or any entity with a domain name server to remove or disable computer data that is being stored or transmitted in contravention of the Act;

- ✓ would empower the Court to make an order to produce information relating to computer data that is required for a criminal investigation or criminal proceedings;

- ✓ would empower a Magistrate to order the expedited preservation of computer data if he has reasonable grounds to believe that the data is susceptible to modifications;

- ✓ would impose liability on an internet service provider who intentionally and without lawful excuse, discloses the details of an Order of a Court;

- ✓ would give authority to a Magistrate, who has reasonable grounds to believe that data stored in a computer system is required for a criminal investigation, to order the partial disclosure of traffic data;

- ✓ provides that a Magistrate may authorize a police officer to utilize remote forensic tools[7] if he reasonably believes that evidence cannot be collected without the use of such tools. The schedule to the Act would stipulate the offences for which these tools may be used. These are:

    - offences involving treason under the Treason Act, Chap. 11:03 ;
    - offences against the person namely, murder and manslaughter;
    - offences involving kidnapping;
    - drug trafficking, namely trafficking in dangerous drugs and possession of a dangerous drug for the purpose of trafficking;
    - unlawful possession of a firearm or ammunition;
    - offences involving a terrorist act;
    - trafficking in persons or trafficking in children;
    - offences involving child pornography; and
    - offences involving fraud.

- ✓ would empower the Court to order payment of an additional fine where monetary benefits were gained as a result of the commission of an offence under the Act or where loss or damage was caused as a result;

- ✓ would empower the Court to order payment of compensation for loss or damage suffered as a penalty for offences under the Act and the procedure for making an application for such compensation;

[7] Remote forensic tools refer to 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. Taken from the Cybercrime Bill 2014. Pgs. 3-4.

- ✓ would provide the procedure for the Court to make a forfeiture order and the treatment of property forfeited as it relates to any property used for or in connection with, or obtained as proceeds from the commission of an offence under the Act;

- ✓ would empower the Court to issue a warrant for the search and seizure, and a restraint order to prohibit the disposal of any property that is to be forfeited under the Act;

- ✓ provides that an internet service provider is not under an obligation to monitor the information which it transmits or stores on behalf of another person or to actively seek facts or circumstances which would indicate illegal activity. Also seeks to prohibit an internet service provider from refusing to comply with any order of the Court or other legal requirement;

- ✓ provides that an access provider is not criminally liable for providing access to or transmitting information prohibited by the Act under the following circumstances:

    - "if he does not initiate the transmission;
    - select the receiver of the transmission; or
    - select or modify the information contained in the transmission"[8].

- ✓ provides that a hosting provider is not criminally liable for the storage of information prohibited by the Act under the following circumstances:

    - "if 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
    - 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 content"[9].

[8] Clause 37 (1) of the Trinidad and Tobago Cybercrime Bill, 2014. Pg. 21.
[9] Clause 38 (1) (a) and (b) of the Trinidad and Tobago Cybercrime Bill, 2014. Pg. 22.

- ✓ provides that a caching provider is not criminally liable for storing information prohibited by the Act under the following circumstances:

    - "if he does not modify the stored information;
    - if he complies with the condition of access to the stored information;
    - if he updates stored information in accordance with any written law or in a manner that is widely recognized and used in the information communication technology industry; or
    - if 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
    - the stored information at the initial source of the transmission has been removed from the network;
    - access to the stored information has been disabled; or
    - a Court has ordered the removal or disablement of the stored information."[10]

- ✓ provides that an internet service provider is not criminally liable for enabling access, via electronic hyperlink, to information provided by another person in contravention of the Act under the following circumstances:

    - "if 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
    - if 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."[11]

[10] Clause 39 (1) (a) to (g) of the Trinidad and Tobago Cybercrime Bill, 2014. Pg. 23.
[11] Clause 40 (1) (a) and (b) of the Trinidad and Tobago Cybercrime Bill, 2014. Pg. 23.

- ✓ provides that a search engine provider who creates an index of internet-related content or makes available electronic tools to search for information is not criminally liable if he does not initiate the transmission, select the receiver of the transmission or select or modify the information contained in the transmission;

- ✓ makes provision for the definition of the term "child offender" under the Act to mean a child who is convicted of an offence under this Act;

- ✓ would impose lower penalties for offences that are committed by child offenders under the Act;

- ✓ would empower the Court to impose liability on a parent or guardian with responsibility for a child offender;

- ✓ would provide for certain matters which the Court may take into account before sentencing a child offender;

- ✓ provides the Minister of National Security with the power to make Regulations for the proper administration of the Act; and

- ✓ would repeal the Computer Misuse Act, Chap: 11:17.

CONSIDERATIONS

The Bill:

- ✓ provides for the creation of offences related to cybercrime in Trinidad and Tobago;

- ✓ makes computer related forgery an offence;

- ✓ shall have effect although it is inconsistent with sections 4 and 5 of the Constitution;

- ✓ has to be supported by a three-fifths majority in each House;

- ✓ makes it an offence to illegally access a computer system as well as to illegally remain logged in a computer system;

- ✓ makes it an offence for persons to intentionally and without lawful excuse, interfere with data, be it alteration, deletion, copies, and movement to a computer storage device or to a different location within a computer system etc.;

- ✓ makes the illegally acquisition of data an offence;

- ✓ does not make reference to the provisions of the Data Protection Act 2011;[12]

- ✓ makes computer related fraud an offence;

- ✓ does not provide a definition of the term 'cybercrime'. However, a definition is provided in the Trinidad and Tobago Cyber Security Agency Bill, 2014;

- ✓ does not provide a definition for the term *'identity theft'*.

- ✓ makes it an offence to violate a person's privacy through the capture, storage, publishing or transmission through a computer system, the image of the private area of another person without his/her consent;

- ✓ makes it an offence to harass a person through electronic communication;

- ✓ adopts the definition of a 'child' that is stated in the Children Act, 2012;[13]

[12] The Data Protection Act 2011 is awaiting proclamation. Click to view http://www.ttparliament.org/legislations/a2011-13.pdf

[13] The Children Act 2012 (Act No. 12 of 2012) is awaiting proclamation. Click to view http://www.ttparliament.org/legislations/a2012-12.pdf

- ✓ modifies the definition of 'Child Pornography' stated in the Children Act.

- ✓ makes provision for the possible payment of an additional fine in an instance where the Court is satisfied that monetary benefits accrued to the person as a result of the commission of the offence. This fine can be in an amount equal to the amount of the monetary benefits gained by the offender.

- ✓ makes provision for a person convicted of an offence under this Act to pay compensation to another person whom the Court is satisfied has suffered loss or damage as a result of the commission of the offence;

- ✓ makes provision for penalties committed by a child offender under the age of sixteen;

- ✓ makes provision for the Court to hold the parents/guardians with responsibility for a child offender, to pay any fine or penalty imposed on the child once the Court is satisfied that the parent/guardian cannot be found and/or did not contribute or participate in the commission of the offence by neglecting to exercise due care/control of the child offender;

- ✓ does not provide a definition of a 'fit person' in whose care a child offender may be placed. However, in the Children Act, a "fit person" has the meaning assigned to it under section 3 of the Children's Authority Act;

- ✓ does not make provision for a preservation regime for stored communications.

COMPARATIVE LEGISLATION IN OTHER JURISDICTIONS

Country	Legislation	Remarks
United Kingdom	Computer Misuse Act 1990.[14] Police and Justice Act 2006. Sections 35 to 38.[15]	An Act to make provision for securing computer material against unauthorized access or modification; and for connected purposes.[16] This Act includes amendments to the Computer Misuse Act 1990 where the maximum prison sentence under section 1 of the original Act was increased from six months to two years. Additionally section 3 of the Act ('unauthorized modification of computer material') was amended to read 'unauthorized acts with intent to impair or with recklessness as to impairing, operation of computer, etc.' and has a maximum sentence of ten years. There is also an additional section, which concerns 'Making, supplying or obtaining articles for use in computer misuse offences' and this carries a maximum sentence of two years.[17]
Australia	Cybercrime Act 2001.[18] Cybercrime Legislation Amendment Act 2012.[19]	An Act to amend the law relating to computer offences, and for other purposes. The Act covers computer offences and law enforcement powers relating to electronically stored data. An Act to implement the Council of Europe

[14] Computer Misuse Act, 1990. http://www.legislation.gov.uk/ukpga/1990/18/contents/enacted
[15] Police and Justice Act 2006. http://www.legislation.gov.uk/ukpga/2006/48/part/5/crossheading/computer-misuse
[16] Computer Misuse Act, 1990. http://www.legislation.gov.uk/ukpga/1990/18/introduction/enacted
[17] Cybercrime and the law: a review of UK computer crime legislation. (Section: New wine in old bottles). https://www.securelist.com/en/analysis/204792064/Cybercrime_and_the_law_a_review_of_UK_computer_crime_legislation
[18] Cybercrime Act 2001. http://www.comlaw.gov.au/Details/C2004A00937
[19] Australia. Cybercrime Legislation Amendment Act 2012. http://www.comlaw.gov.au/Details/C2012A00120

		Convention on Cybercrime, and for other purposes.
New Zealand	Crimes Amendment Act 2003.[20]	This is an Act to amend the Crimes Act 1961 and contains an entire section on crimes involving computers.
Jamaica	The Cybercrimes Act 2010.[21]	An Act to provide criminal sanctions for the misuse of computer systems or data and the abuse of electronic means of completing transactions and to facilitate the investigation and prosecution of cybercrimes.
Nigeria	Cybercrime Bill, 2013.[22]	An Act to provide for the prohibition, prevention, detection, response and prosecution of cybercrimes and for other related matters.
Singapore	Computer Misuse Act 1993.[23] Computer Misuse and Cyber Security Act (Chapter 50A).[24]	An Act to make provision for securing computer material against unauthorized access or modification and for matters related thereto. An Act to make provision for securing computer material against unauthorized access or modification, to require or authorize the taking of measures to ensure cybersecurity, and for matters related thereto.

References

Australia. Cybercrime Legislation Amendment Act 2012.
http://www.comlaw.gov.au/Details/C2012A00120

[20] New Zealand Crimes Amendment Act 2003.
http://www.legislation.govt.nz/act/public/2003/0039/latest/DLM199766.html
[21] Jamaica Cybercrimes Act 2010.
http://www.japarliament.gov.jm/attachments/341_The%20Cybercrimes%20Act,%202010.pdf
[22] Nigeria Cybercrime Bill 2013. http://pinigeria.org/download/cybercrimebill2013.pdf
[23] Singapore Computer Misuse Act 1993.
http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A%228a3534de-991c-4e0e-88c5-4ffa712e72af%22%20Status%3Apublished%20Depth%3A0;rec=0
[24] Computer Misuse and Cyber Security Act Chap: 50A.
http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:8a3534de-991c-4e0e-88c5-4ffa712e72af%20%20Status:inforce%20Depth:0;rec=0

Computer Misuse Act, 1990.
http://www.legislation.gov.uk/ukpga/1990/18/introduction/enacted

Computer Misuse Act, 1990. http://www.legislation.gov.uk/ukpga/1990/18/contents/enacted

Computer Misuse and Cyber Security Act Chap: 50A.
http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:8a3534de-991c-4e0e-88c5-4ffa712e72af%20%20Status:inforce%20Depth:0;rec=0

Cybercrime Act 2001. http://www.comlaw.gov.au/Details/C2004A00937

Cybercrime and the law: a review of UK computer crime legislation. (Section: New wine in old bottles).
https://www.securelist.com/en/analysis/204792064/Cybercrime_and_the_law_a_review_of_UK_computer_crime_legislation

Electronic Transactions Act, 2011. http://www.ttparliament.org/legislations/a2011-06.pdf

Government of Trinidad and Tobago National Cyber Security Strategy. 2012. Pgs. 1-4.
http://www.nationalsecurity.gov.tt/Portals/0/Pdf%20Files/National_Cyber_Security%20Strategy_Final.pdf

Interception of Communications Act, 2010.
https://www.ttbizlink.gov.tt/trade/tnt/cmn/pdf/Interceptions%20Act.pdf

Jamaica Cybercrimes Act 2010.
http://www.japarliament.gov.jm/attachments/341_The%20Cybercrimes%20Act,%202010.pdf

New Zealand Crimes Amendment Act 2003.
http://www.legislation.govt.nz/act/public/2003/0039/latest/DLM199766.html

Nigeria Cybercrime Bill 2013. http://pinigeria.org/download/cybercrimebill2013.pdf

Police and Justice Act 2006.
http://www.legislation.gov.uk/ukpga/2006/48/part/5/crossheading/computer-misuse

Cybercrime Bill, 2014. Trinidad and Tobago. Clauses 37 (1), 38 (1) (a) and (b), 39 (1) (a) to (g), and 40 (1) (a) and (b). Pgs. 21-23.
http://www.ttparliament.org/legislations/b2014h05.pdf

Singapore Computer Misuse Act 1993.
http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A%228a3534de-991c-4e0e-88c5-4ffa712e72af%22%20Status%3Apublished%20Depth%3A0;rec=0

The Community Service Orders Act.
http://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/13.06.pdf

The Treason Act Chap. 11:03.
http://rgd.legalaffairs.gov.tt/laws2/alphabetical_list/lawspdfs/11.03.pdf

Webopedia. Cybercrime. http://www.webopedia.com/TERM/C/cyber_crime.html

Parliament Secretariat
Parliament of the Republic of Trinidad and Tobago
Levels G-7, Tower D,
Port of Spain International Waterfront Centre
#1A Wrightson Road, Port of Spain
TRINIDAD