PARLIAMENT
REPUBLIC OF TRINIDAD AND TOBAGO

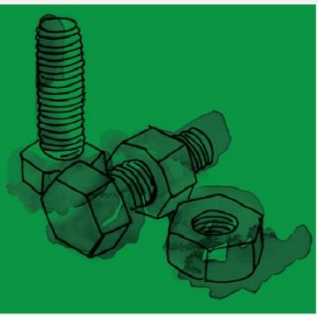
Secretariat Unit

# Bill Essentials

## The Cybercrime Bill, 2015

**An Act to to provide for the creation of offences related to cybercrime and for other related matters in Trinidad and Tobago**

Bill No: HOR Bill 7 of 2015
Introduced in: The House of Representatives
Introduced on: May 1, 2015
Introduced by: Sen. Hon. Brig. Gen. Alfonso [Minister of National Security]



# Contents

## Background

The Cybercrime Bill, 2015[1] was introduced and read for a first time in the House of Representatives on May 1, 2015 by Senator the Hon. Brig. Gen. Alfonso, Minister of National Security. A previous incarnation of this Bill was introduced[2] [3]during the 4th Session of the 10the Parliament, however it lapsed. This Bill should be read together with the Trinidad and Tobago Cyber Security Agency Bill, 2015.[4]

## Purpose of the Bill

The Bill seeks to provide for the creation of offences related to cybercrime and for other related matters in Trinidad and Tobago. The Bill is comprised of forty-two (42) clauses and one (1) Schedule.

## Legislation mentioned in the Bill

Computer Misuse Act Chap. 11:17[5]
Electronic Transactions Act Chap. 22:05[6]
Interception of Communications Act Chap. 15:08[7]
Treason Act Chap. 11:03[8]

## Key Features of proposed Legislation

1. Clause 1 provides for the short title.
2. Clause 2 would provide for the Act to come into operation on Proclamation by the President.
3. Clause 3 provides that the Act shall have effect though inconsistent with the Constitution.
4. Clause 4 would define certain terms used in the Bill.
5. Clause 5 seeks to create the offence of illegally accessing a computer system. 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.
6. Clause 6 seeks to create the offence of illegally remaining in a computer system which 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.
7. Clause 7 seeks to create the offence of illegally intercepting non- public transmission or electromagnetic emissions to, or from a computer system. This offence would carry a fine of two hundred and fifty thousand dollars and imprisonment for three years on summary conviction or a fine of five hundred thousand dollars and five years' imprisonment on conviction on indictment.

[1] http://www.ttparliament.org/legislations/b2015h07.pdf
[2] http://www.ttparliament.org/legislations/b2014h05g.pdf
[3] http://www.ttparliament.org/documents/2240.pdf
[4] http://www.ttparliament.org/legislations/b2015h08.pdf
[5] http://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/11.17.pdf
[6] http://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/22.05.pdf
[7] http://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/15.08.pdf
[8] http://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/11.03.pdf

8. Clause 8 seeks to create the offence of illegally interfering with computer data and 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.
9. Clause 9 seeks to create the offence of illegally acquiring computer data whether for personal use or for use by another person. This 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.
10. Clause 10 seeks to create the offence of illegally interfering with a computer system or a person who is 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.
11. Clause 11 seeks to impose greater penalties on persons who commits an offence under Part II and which affects critical infrastructure. This clause would define "critical infrastructure" 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. An offence under this clause would carry a penalty of two million dollars and fifteen years' imprisonment on conviction on indictment.
12. Clause 12 seeks to create the offence of illegally producing, selling, procuring, importing, exporting, distributing or otherwise making available a computer device or program 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.
13. Clause 13 seeks to create the offence of 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.
14. Clause 14 seeks to create the offence of computer-related forgery. This would make it unlawful to input, alter, delete or suppress computer data which would result in inauthentic data 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.
15. Clause 15 seeks to create the offence of computer-related fraud and 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.

16. Clause 16 seeks to create the offence of identity theft through the use of a computer system which 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.
17. Clause 17 seeks to create 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.
18. Clause 18 seeks to create the offence of violating a person's privacy by capturing and sharing pictures or videos of a person's private area without his consent. This 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.
19. Clause 19 seeks to criminalise 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.
20. Clause 20 seeks to create the offence of 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.
21. Clause 21 would provide for the jurisdiction of the Courts of Trinidad and Tobago as it would relate to its territorial limits under the Act.
22. Clause 22 would impose liabilities for offences committed by a body corporate or any person purporting to act in such capacity.
23. Clause 22 would impose liabilities for offences committed by a body corporate or any person purporting to act in such capacity.
24. Clause 24 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.
25. Clause 25 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.
26. Clause 26 would empower the Court to make a production order relating to computer data that is required for a criminal investigation or criminal proceedings.
27. Clause 27 empowers a Magistrate to order the expedited preservation of computer data if he has reasonable grounds to believe that the data is susceptible to modifications.
28. Clause 28 would impose liability on an internet service provider who intentionally and without lawful excuse discloses the details of an Order of a Court.

29. Clause 29 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.
30. Clause 30 would provide that a Magistrate may authorize a police officer to utilize remote forensic tools 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.
31. Clause 31 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.
32. Clause 32 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.
33. Clause 33 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.
34. Clause 34 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.
35. Clause 35 would provide 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. This clause also seeks to prohibit an internet service provider from refusing to comply with any order of the Court or other legal requirement.
36. Clause 36 would provide that an access provider is not criminally liable for providing access to, or transmitting information prohibited by the Act under certain circumstances.
37. Clause 37 would provide that a hosting provider is not criminally liable for the storage of information prohibited by the Act under certain circumstances.
38. Clause 38 would provide that a caching provider is not criminally liable for storing information prohibited by the Act under certain circumstances.
39. Clause 39 would provide 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 certain circumstances.
40. Clause 40 would provide 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.
41. Clause 41 would give the Minister the power to make Regulations for the proper administration of the Act.
42. Clause 42 would repeal the Computer Misuse Act, Chap. 11:17.

## Considerations

- The Bill provides that a child means a person under the age of eighteen (18) years as opposed to fourteen (14) as specified in the Children Act 2012.[9]
- The Bill does not define 'cybercrime' however, it is defined in the Trinidad and Tobago Cyber Security Agency Bill, 2015[10]
- The offence created by clause 17 appears to be in conflict with offences created by section 7 and 8 of the Sexual Offences Act Chap. 11:28.[11]
- The Bill makes it an offence to violate a person's privacy by capturing and sharing pictures and/or videos of a person's private area without his consent.
- The Bill provides that the Court may order an additional fine for an offence committed if monetary benefits were gained as a result of the offence.
- The Bill provides the internet service providers may be subject to a production order during the course of criminal investigations or criminal proceedings.

## Comparative Legislation in other Jurisdictions

| Country | Legislation | Remarks |
|---|---|---|
| **United Kingdom** | Computer Misuse Act 1990[12] | An Act to make provision for securing computer material against unauthorized access or modification; and for connected purposes |
| **Australia** | Cybercrime Act 2001[13]<br><br>Cybercrime Legislation Amendment Act 2012[14] | 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.<br><br>An Act to implement the Council of Europe Convention on Cybercrime, and for other purposes |

[9] http://www.ttparliament.org/legislations/a2012-12.pdf
[10] http://www.ttparliament.org/legislations/b2015h08.pdf
[11] http://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/11.28.pdf
[12] http://www.legislation.gov.uk/ukpga/1990/18/introduction/enacted
[13] http://www5.austlii.edu.au/cgi-bin/download.cgi/cgi-bin/download.cgi/download/au/legis/cth/consol_act/ca2001112.rtf
[14] http://www.austlii.edu.au/cgi-bin/download.cgi/cgi-bin/download.cgi/download/au/legis/cth/num_act/claa2012304.rtf

| | | |
|---|---|---|
| **New Zealand** | Crimes Amendment Act 2003[15] | This is an Act to amend the Crimes Act 1961 and contains an entire section on crimes involving computers. |
| **Jamaica** | The Cybercrimes Act 2010[16] | 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[17] | An Act to provide for the prohibition, prevention, detection, response and prosecution of cybercrimes and for other related matters. |
| **Singapore** | Computer Misuse Act 1993[18] | An Act to make provision for securing computer material against unauthorized access or modification and for matters related thereto. |
| | Computer Misuse and Cyber Security Act (Chapter 50A)[19] | 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. |

# Reference Material

### Articles


- United Nations Office on Drugs and Crime. Comprehensive study on Cybercrime. February 2013. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

- McAfee. Centre for Strategic and International Studies. July 2013. The Economic Impact of Cybercrime and Cyber Espionage. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

- Neal K. Katyal *Criminal Law in Cyberspace,* 149 U. Pa. L. Rev. 1003 (2001). http://scholarship.law.upenn.edu/penn_law_review/vol149/iss4/2


[15] http://www.legislation.govt.nz/act/public/2003/0039/latest/DLM199766.html
[16] http://www.japarliament.gov.jm/attachments/341_The%20Cybercrimes%20Act,%202010.pdf
[17] https://www.pinigeria.org/download/cybercrimebill2013.pdf
[18] 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
[19] 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

- Cybersecurity and Cybercrime. Presented by Ministry of National Security. http://chamber.org.tt/wp-content/uploads/2013/09/Cybersecurity-and-Cybercime-presented-by-the-Ministry-of-National-Security.pdf

- Council of Europe. Cybercrime Legislation – country profiles. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp


**Newspaper References**


- Trinidad and Tobago Newsday, June 14, 2014 - Online bullying a major cyber-crime http://www.newsday.co.tt/news/0,196225.html

- Trinidad Express Newspapers, June 13, 2014 – Hackers Beware http://www.trinidadexpress.com/news/Govt-tackling-mailbox-politics--263115491.html

- Panapress, October 24, 2014 - Nigeria: Nigerian Senate passes law to curb cybercrime, online fraud http://www.panapress.com/Nigeria--Nigerian-Senate-passes-law-to-curb-cybercrime,-online-fraud---13-630407675-0-lang4-index.html


Parliament Secretariat
Parliament of the Republic of Trinidad and Tobago
Levels G-8, Tower D,
Port of Spain International Waterfront Centre
#1A Wrightson Road, Port of Spain
TRINIDAD
**May 13, 2015**