Trinidad and Tobago Perspective- Drafting of Cybercrime Legislation

PRESENTED BY:

SUNITA RAMSUMAIR

LEGAL OFFICER II

MINISTRY OF NATIONAL SECURITY

Format of the Presentation

- History of the Cybercrime Bill
- Concerns with the Cybercrime Bill, 2014
- Cybercrime Bill, 2015
- Concerns with the Cybercrime Bill, 2015
- Where are we now?
- Lessons Learnt

History of the Cybercrime Bill

- Trinidad and Tobago was a beneficiary of the ITU HIPCAR Project -Enhancing competitiveness in the Caribbean through the harmonisation of ICT Policies, Legislation and Regulatory Procedures

- Reviewed other precedents including:
  - Council of Europe Convention on Cybercrime,
  - The ITU Global Protocol on Cybersecurity and Cybercrime- The Chairman's Model Law for Cybercrime Legislation, 2009
  - The Netherlands Criminal Code,
  - Cybercrime Act 2010, Jamaica,
  - Cybercrime Prevention Act, Republic of Philippines

History of the Cybercrime Bill

- Creation of additional offences not contained in the HIPCAR Model Legislations, as well as in the COE Convention on Cybercrime:
  - Unauthorised receiving or granting of access to computer data
  - Luring
  - Violation of Privacy (Voyeurism)
  - Expansion of Harassment utilizing electronic communication to include Cyberbullying, as well as, the dissemination of information with the intent to damage a persons reputation.

- The Cybercrime Bill, 2014 was introduced into Parliament in March 2014 and subsequently lapsed in July 2014

Concerns with the Cybercrime Bill, 2014

- Members of the Opposition, as well as the Trinidad and Tobago Publishers and Broadcasters Association (TTPBA), stated that certain clauses in the Cybercrime Bill infringed on the constitutional rights of freedom of press and freedom of speech.
  - The Ministry in response deleted namely sub-clauses 21(2) and 21(3).
    - Sub-clause 21(2)- A person who uses a computer system to disseminate any information, statement or image, knowing the same to be false, and who –

      (a) damages the reputation of another person; or

      (b) subjects another person to public ridicule, contempt, hatred or embarrassment,

      commits an offence.
    - Sub-clause 21(3) -(3) A person who intentionally or recklessly –

      (a) uses a computer system to disseminate any information, statement or image; and

      (b) exposes the private affairs of another person, thereby subjecting that other person to public ridicule, contempt, hatred or embarrassment,

      commits an offence.

Concerns with the Cybercrime Bill, 2014

- Further, it was believed that the clauses relating to Child Pornography and Luring in the Cybercrime Bill, 2014 were similar to clauses in the Children Act, 2012 and the clauses in the Cybercrime Bill carried a higher penalty than those in the Children Act, 2012.
  - The Ministry in response held a meeting with the then Ministry of Gender, Youth and Child Development and it was recommended and accepted that these offence be removed together with Part V- Child Offenders. Those amendments were made on the floor by the then Minister of National Security during the debates on the Cybercrime Bill, 2014.

Cybercrime Bill, 2015

- The Cybercrime Bill, 2015 was introduced into Parliament in May 2015 with the following changes:
  - The offence of child pornography was removed;
  - The offence of luring was re-introduced;
  - Part V- Child Offenders was removed;
  - Sub-clauses 21(2) and (3) were removed; and
  - New penalties for all crimes: $1M and 3 years and $2M and 5 years, save and except Offences against Critical Infrastructure which was increased from $2M to $5M and Computer Related Forgery which was increased from $20,000 to $1M.

- The Cybercrime Bill, 2015 lapsed in June 2015

Concerns with the Cybercrime Bill, 2015

- Clause 9- Illegal acquisition of data. The Media Associations were of the view that this clause impacts on their ability to engage in investigative journalism, as it criminalizes the unauthorized access to computer data. The Media Associations further indicated that there is no definition of 'unauthorized access' and highlighted the option of limiting the information solely to national security data or the possibility of allowing for the disclosure of certain types of information. The Media Associations indicated that the clause should be deleted in its entirety. It was discussed that acquisition of specially protected data should be criminalized under other data-specific legislation.
- Clause 13- Unauthorized receiving of data. The Media Associations indicated that they wanted this deleted for similar reasons given for Clause 9.
- Clause 22- Offence by Body Corporate. The Media Associations were of the opinion that there should be a media exemption, as there is a clear distinction between the newsroom and the executive management given that the executive management did not want to be liable for the work of the newsroom as they have no control in the newsroom.

Where are we now?

- Prior to the Cybercrime Bill, 2015 lapsing, a meeting was held with executive of the then Government and the Media Associations to better understand the concerns of the Media.
- In 2015 the administration for the Government changed
- In 2016 the Attorney General engaged the Media in further consultations with a view to hearing their concerns and invited them to submit proposed alternative clauses
- At this time the Ministry of National Security as well as the Ministry of the Attorney General and Legal Affairs are in on-going consultations with the Media Associations

Lessons Learnt (thus far)

- Multi-stakeholder Approach
- Political Will
- Consultation and Consensus

Thank You

Sunita Ramsumair

Legal Officer II

sramsumair@mns.gov.tt

Ministry of National Security

Government of the Republic of Trinidad and Tobago