AGC SINGAPORE | ATTORNEY-GENERAL'S CHAMBERS

OCTOPUS CONFERENCE

11-13 July 2018, Strasbourg

Workshop 2 – The Global State of Cybercrime Legislation

Creating and maintaining a strong legal framework to combat cybercrime: The Singapore Experience

G. Kannan
Senior Director,
Technology Crime Unit,
Financial & Technology Crime Division
Attorney-General's Chamber, Singapore.

Substantive Criminal Law

Law of Criminal Procedure

Law of Evidence

AGC SINGAPORE | ATTORNEY-GENERAL'S CHAMBERS

SUBSTANTIVE LAW

- Computer Misuse & Cybersecurity Act ("CMCA")
  - Singapore's primary cybercrime legislation
  - Focuses on computer integrity crimes
  - Enacted in 1993 – borrowed from UK and Australian legislation
  - Predates the Budapest Convention but Singapore law is favourably aligned with the legal requirements of the Convention, though not a signatory
  - Core offences are mirrored in the Convention (illegal access / interception / data interference etc)
  - Core offences in CMCA (1st gen computer crimes) *remain* completely applicable today

- Best practices :
  - Important to have a strong set of baseline computer crime offences
  - Be guided by legislation from other countries / international instruments – adopt what works
  - Harmonisation of laws across countries is key!
  - Craft laws in technologically-neutral terms to ensure they remain applicable to rapidly evolving technologies and patterns of criminal behaviour.

SUBSTANTIVE LAW

- Computer Misuse & Cybersecurity Act
  - Amended in 1998, 2005, 2008, 2013 and recently in 2017
  - 2008: introduced 2nd gen computer crimes (e.g system interference a.k.a unauthorised obstruction)
  - 2017: further aligned with criminal offences in Convention by introduction of offence criminalising possession / supply of hacking tools
  - 2017: provides jurisdiction over cybercrimes committed *overseas*, against *overseas* computers, which create a significant risk of serious harm in Singapore

- Best practices:
  - Agile responses are needed to combat the evolving threat of cybercrime
  - Scope of laws must be expanded to tackle the increasing scale and transnational nature of online crimes

SUBSTANTIVE LAW

2017 : New offence on obtaining, retaining or supplying personal information obtained through cybercrime

- New section 8A - criminalises possession / use / supply of personal information obtained illegally (e.g., through illegal access), where the person knows or has reason to believe that the personal information was obtained illegally.
- To prove the person's knowledge that the information was obtained in breach of the CMCA, the prosecution does not have to prove the particulars of the contravention, such as who carried out the contravention and when it took place.

- Best practice:
  - Identify and fill gaps in the law which allows offending conduct to go unpunished; which targets other actors in the cybercrime ecosystem
  - Keep cybercrime laws under review, to ensure legal frameworks take account of developments

NEW SECTION 39 OF THE CPC

Expansion of law enforcement power to access computer data

- Law enforcement now empowered to access and copy evidence on computers regardless of whether the evidence is stored on a computer inside or outside Singapore.

- Section 39 CPC - Power to access computer
  - A police officer may
  - Access a computer (whether in Singapore or elsewhere)
  - That is reasonably suspected of :
    - ❖ being used in connection with an offence; or
    - ❖ containing evidence relating to the offence.

- Power extends to searching any data contained in / available to such computers; and to make a copy of any such data.

NEW SECTION 39 OF THE CPC

Expansion of law enforcement power to access computer data

- Investigators may conduct remote search if the computer is known to be outside Singapore or if its whereabouts are unknown, where
  - the owner of that computer consents to the search;
  - the owner of that data consents to the search;
  - the access is obtained through an active connection with another computer, which has been lawfully seized;
  - the access is obtained through any username, password or other authentication information stored in another computer, which has been lawfully seized; or
  - the access is obtained through any username, password or other authentication information provided in any statement made by any person during investigations.

NEW SECTION 39 OF THE CPC

Expansion of law enforcement power to access computer data

- Investigators are also empowered to order a person to provide login credentials to a computer or a cloud services account.

- The investigator may order any of the following persons to provide the necessary assistance:
  - any person whom the police officer reasonably suspects of having used the computer in connection with the offence;
  - any person concerned with the operation of the computer;
  - any person whom the police officer reasonably believes has knowledge of any login credentials to the computer.

- The types of assistance that can be sought?
  - assistance to gain access to the computer (including assistance through the provision of any username, password or other authentication information required to gain access to the computer)

Looking ahead …

- Challenge posed by virtual currencies
  - Criminal laws that hinge on the concept of property must be reviewed
  - Amendments to Singapore law scheduled in 2019

- Challenge posed by Artificial Intelligence and autonomous systems
  - Who will the law hold liable?
  - Can the law hold anyone liable?