AGC SINGAPORE | ATTORNEY-GENERAL'S CHAMBERS

Legislative Framework for Fighting Cybercrime

The Singapore Experience

Christopher SJ ONG
Senior Director, Commercial and Technology Crimes
Crime Division, Attorney-General's Chambers

Introduction

- What is Cybercrime?
  - Computer integrity crimes
  - Computer-facilitated crimes
  - Content crimes

E-Commerce Scams

2017 1,907 Cases
2018 2,125 Cases
↑ 11.4%

2018 Total Amount Cheated **$1.9 million** | Highest Amount Cheated **Close to $69,000**

Loan Scams

2017 396 Cases
2018 994 Cases
↑ 151.0%

2018 Total Amount Cheated **$2 million** | Highest Amount Cheated **Close to $90,000**

Internet Love Scams

2017 826 Cases
2018 660 Cases
↓ 20.1%

2018 Total Amount Cheated **$27.5 million** | Highest Amount Cheated **Close to $1.3 million**

Scams of Concern

E-Commerce Scams

2017 1,907 Cases
2018 2,125 Cases
↑ 11.4%

2018 Total Amount Cheated **$1.9 million** | Highest Amount Cheated **Close to $69,000**

Loan Scams

2017 396 Cases
2018 994 Cases
↑ 151.0%

AGC SINGAPORE | ATTORNEY-GENERAL'S CHAMBERS

What is Cybercrime?

- Increasingly, the challenge is computer-facilitated crimes
  - ”Old wine in new bottles”
  - Every crime = cybercrime?
- Legislative framework must be:
  - Holistic
  - Regularly reviewed and updated
- Also need to address operational challenges

Legislative responses

- Cybercrime-specific legislation
- Updated Traditional Criminal Law
- Procedural Legislation
  - Investigative Powers
  - Admissibility of Evidence

Cybercrime-specific legislation

- Computer Misuse Act
  - Computer-integrity crimes
  - Updated in 2017 to introduce new crimes:
    - Possession etc. of personal information
    - Possession etc. of hacking tools

- Remote Gambling Act
  - Online gambling

- Protection from Online Falsehoods and Manipulation Bill
  - Anti-fake news law

Updated traditional legislation

- Penal Code
  - Updated in 2007 to include electronic forms of certain traditional crimes
  - Updated most recently in 2018
    - Updated more traditional crimes
    - Cheating etc. of automated systems
    - New offences, including “no outcome” fraud and possession of personal information
    - Updating and introducing new definitions

- Protection from Harassment Act
  - Online harassment
  - Stalking (including cyberstalking)
  - Civil remedies

Police Investigative Powers

- Amendments to Criminal Procedure Code in 2018, to ensure that law enforcement is empowered to access 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.

Police Investigative Powers

- 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.

Police Investigative Powers

- 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)

Admissibility of Evidence

- Pre-2012
  - Law reflected (archaic?) perception that electronic evidence was (inherently) prone to fabrication / tampering.
  - Parties admitting electronic evidence had to establish reliability of the computer system that produced/stored the evidence, before it could be admitted.

- 2012 amendments
  - Evidence Act was amended and additional pre-requisites to admitting electronic evidence were repealed.
  - Electronic evidence is now treated the same way as any other form of evidence.
  - Threshold of admissibility = relevance.
  - Like any other evidence, adverse party can challenge admissibility / reliability

Conclusion