The Legal Frameworks Necessary to Support the Successful Prosecution of Transnational Cybercrimes

Professor Jonathan Clough, Monash University
CyberBayKin: Secure a Digital Myanmar
27 November 2018
➢ Brian May: 7 years, 10 months
➢ Network of 45,000 Members
➢ Shannon McCoole: 35 years (min. 28)
➢ Richard Huckle: 22 life terms (min. 25)
➢ 85 children rescued
➢ 100s of arrests

TASKFORCE ARGOS
Defining ‘Cybercrime’

➢ Cyber-dependent crimes (e.g. hacking);
➢ Cyber-enabled crimes (e.g. fraud); and
➢ Computer-supported crimes (e.g. drug trafficking).
Defining ‘Cybercrime’
A Comprehensive Response to Cybercrime

- Criminal Law
- International Cooperation
- Procedural Law
- Jurisdiction
A COMPREHENSIVE RESPONSE TO CYBERCRIME

- Cybersecurity Policy and Strategy
- Cyber Culture and Society
- Cybersecurity Education, Training and Skills
- Legal and Regulatory Frameworks
- Standards, Organisations, and Technologies

~ Oxford Internet Institute,
Cybersecurity Capacity Maturity Model for Nations
THE COUNCIL OF EUROPE “BUDAPEST” CONVENTION ON CYBERCRIME

➢ The first binding international instrument to comprehensively address the issue of cybercrime.
➢ Opened for signature on 23 November 2001, the Convention entered into force on 1 July 2004.
➢ Signed by 46 of 47 member states of the Council of Europe. Ratified by 43.
➢ Ratified by 18 non-member states. Signed but not ratified by South Africa. A further 6 non-member states invited to sign.
The Budapest Convention

Ratified
The Budapest Convention

Ratified/Signed
The Budapest Convention

Ratified/Signed/Invited
SUBSTANTIVE OFFENCES

➢ Offences against the confidentiality, integrity and availability of computer data and systems
➢ Computer-related offences (fraud/forgery)
➢ Content-related offences (child pornography)
➢ Criminal Copyright Infringement
➢ Additional Protocol concerning acts of a racist and xenophobic nature committed through computer systems
A number of cybercrimes are not included in the Convention. For example:

- Harassment
- Sexual ‘grooming’ of children
- Unsolicited emails: ‘spam’
- ‘Cyberterrorism’
- Identity ‘theft’
Case Study: Identity Theft

➢ ‘Identity’ theft is the acquisition of another person’s identity information. Identity information may then be used to commit other offences.

➢ For example, in *U.S. v Onwuahara* (ED Va, 2013), Onwuahara and his co-conspirators were convicted in relation to total fraud of US$13 million (attempted US$38 million)

➢ Defendants used online databases to identify potential victims and acquire identity information.

➢ They then used other databases to acquire further identity information before contacting banks and impersonating victims.

➢ They were then able to transfer money to domestic and overseas bank accounts.
CASE STUDY: IDENTITY THEFT

Stage One: Acquisition and/or Creation of Identity Information

Stage Two: Possession and Distribution

Stage Three: Use
CASE STUDY: IDENTITY THEFT

Stage One: Hacking

Stage Two: Identify Theft

Stage Three: Fraud
The UN has encouraged member states to ‘consider establishing or updating, as appropriate, criminal offences for the illicit taking, copying, fabrication and misuse of identification documents and identification information.’

However, international surveys show very few countries have specific identity theft laws:

- Objection in principle
- Existing laws are sufficient
- Difficulty of reaching international agreement, particularly on the meaning of ‘identity information’
PROCEDURAL LAWS

➢ Expedited Preservation of Stored Computer Data/Expedited Preservation and Partial Disclosure of Traffic Data
➢ Production Orders
➢ Search and Seizure of Stored Computer Data
➢ Real-time Collection of Traffic Data
➢ Interception of Content Data
CASE STUDY: MODERN SEARCH POWERS

➢ Traditional warrants were based on physical property: ‘search seize and carry away’. They may not be suitable for modern digital searches.

➢ Compare with s. 3L Crimes Act 1914 (Cth): “The executing officer may operate electronic equipment at the warrant premises to access data (including data not held at the premises) if he or she suspects on reasonable grounds that the data constitutes evidential material.”
CASE STUDY: MODERN SEARCH POWERS

Surveillance Devices Act 1999 (Vic):
➢ ‘Data surveillance device’ means ‘any device capable of being used to record or monitor the input of information into or the output of information from a computer...’.
➢ ‘Device’ includes ‘instrument, apparatus and equipment’

Surveillance Devices Act 2004 (Cth):
➢ ‘Data surveillance device ’ means ‘any device or program capable of being used to record or monitor....’.
Part 5 Investigatory Powers Act 2016 (UK)

Equipment interference operations may involve:

➢ covertly downloading data from a subject’s mobile device when it is left unattended

➢ using login credentials to gain access to data held on a computer

➢ exploiting existing vulnerabilities in software in order to gain control of devices or networks

Case Study: Data Retention

- Available powers and levels of protection typically vary according to the type of data: e.g. ‘traffic data’ vs ‘content’ data.
- ‘Metadata’ is data that relates to other data. May include: identity, source, destination, date, time, duration, type of service (email, SMS, etc), location.
- Australia requires telecommunication providers to store customer metadata for 2 years.
- Such schemes have been subject to challenge in other jurisdictions, such as Europe, as being contrary to privacy and other rights.
Encryption
A number of jurisdictions have provisions allowing for a person to be compelled to provide a password/encryption key.

For example, in Australia, an order compelling production may be made. Failure to comply carries a maximum of 2 years’ imprisonment: s. 3LA Crimes Act 1914 (Cth).

Such provisions have faced challenges in some jurisdictions, such as the United States, on the basis that they violate the protection against self-incrimination.
‘In line with the expectations of our peoples we also encourage collaboration with industry to provide lawful and non-arbitrary access to available information where access is necessary for the protection of national security against terrorist threats. We affirm that the rule of law applies online as well as it does offline.’

-G20 Leaders’ Statement on Countering Terrorism, 7 July 2017
CASE STUDY: REMOTE ACCESS

➢ US authorities investigating the ‘PlayPen’ Child Exploitation network with over 150,000 members.
➢ As it was a DarkNet network it was not possible to locate users.
➢ Server was identified and seized.
➢ Use of ‘Network Investigative Techniques’ under warrant allowed law enforcement to access IP addresses.
➢ Such techniques have been challenged as extraterritorial searches (e.g. US v Gaver (SD Ohio, 2017))
Sovereignty
Sovereignty
CASE STUDY: TRANSBORDER SEARCH

➢ Warrant served on U.S. branch office of a Microsoft subsidiary in Ireland, seeking content stored in Ireland but accessible at the U.S. branch
➢ Account opened and established in Ireland by an Irish citizen. The disclosure would arguably breach Irish law
➢ U.S. law enforcement could request the content through MLAT
➢ Now addressed by Clarifying Lawful Overseas Use of Data (‘CLOUD) Act

~ In the Matter of a Warrant to Search a Certain E-Mail Account v US, 855 F.3d 53 (2nd Circ., 2017)
BUDAPEST CONVENTION ART. 32

➢ Allows trans-border access to stored data where:
  ➢ Publicly accessible; or
  ➢ With lawful and voluntary consent

➢ Other forms of search are neither authorised nor precluded (e.g. Ivanov/Gorshkov).
EXTRADITION: THE ‘LOVE BUG’ VIRUS

➢ The virus first appeared in Hong Kong in 2000 and then spread rapidly throughout the world.
➢ The virus was estimated to have affected over 45 million users including government agencies in more than twenty countries, allegedly causing billions of dollars in damage.
➢ Although investigators were able to determine that the person responsible was a former computer-science student in the Philippines, as the Philippines had no applicable law punishing such conduct he could not be extradited to the United States due to the lack of dual criminality.
EXTRADITION: DUAL CRIMINALITY

➢ ‘Extradition is the formal surrender by one state, on request of another state, of a person who has been accused or convicted of a crime committed within the requesting state’s jurisdiction.’

➢ Extradition is a matter of international comity rather than an obligation under international law. It is usually treaty based.

➢ The COE Convention contains the principle “extradite or prosecute”.

➢ Dual criminality is usually satisfied so long as the conduct is criminalised in both jurisdictions, and is punishable at a defined level (e.g. at least 12 month’s imprisonment). It is not necessary for the offence to be criminalised in the same way.
HARMONISATION ≠ IDENTICAL

International (e.g. Budapest Convention, UNCTOC)
Regional
HARMONISATION

1. Acknowledge the importance of harmonization of laws related to cybercrime and electronic evidence;
2. Encourage ASEAN Member States to explore the feasibility of acceding to existing regional and international instruments in combating cybercrime;

~ ASEAN Declaration to Prevent and Combat Cybercrime, 13 November 2017
HARMONISATION ≠ IDENTICAL

International (e.g. Budapest Convention, UNCTOC)
Regional
Bi-lateral
Agency-agency
24/7/CERTs
Disruption
Prevention
Disruption
Enforcement
“Overall, the global picture is one of a certain degree of fragmentation...”

Source: draft UNODC Comprehensive Study on Cybercrime 2013
Thank you
jonathan.clough@monash.edu