# IT LAW EXAMINABLE CONTENT

## COMPUTER CRIME: Context and Legislation

Computer crime definition:

- Any criminal activity involving an information technology infrastructure
- Traditional crimes are now able to occur via the internet, internet merely facilitates these crimes
- Crimes unique to the internet and computers
- E.g. theft from hacking banks, cyber-bullying, scamming, phishing (imitating a trusted site), stealing credentials and logins, identity theft, virus spreading, terrorism, information warfare, cyber-security for corporates and govt, stock market manipulation, theft of IP, piracy

Territoriality

- Territoriality is a feature of the criminal justice system in Aus which affects the ability to tackle computer misuse. This is because each jurisdiction in Aus has its own separate criminal law
- International nature of computer crimes further aggravates this problem, with Intl jurisdictions causing headaches for regulators
- Key response to this challenge is an Intl attempt to obtain consistent laws across the world. However it still does not deal with the challenges of prosecuting offshore perpetrators.

Challenge for regulators

- Anonymity (encrypt things, disguise identity)
- Global reach (incl. issues of jurisdiction, disparate criminal laws and the potential for large scale victimisation)
- Speed at which crimes can be committed (very fast)
- Potential for deliberate exploitation of sovereignty issues and cross-jurisdictional differences by criminals and organised crime
- Volatility or transient nature of evidence, incl. no collateral or forensic evidences such as eyewitnesses, fingerprints or DNA
- High costs of investigations

Existing offences (if no legislation)

- Fraud – the problem of computerised consent

- Telecommunications offences (eavesdropping on telephone calls)
- Theft in information (selling confidential info to major banks → but is info 'property'?)
- Theft of copyright (different to infringing copyright)
- Destruction or damage to info or data stored on comp (hard to trace)

Cybercrime Act 2001

- An important step toward achieving Intl. consistency and remedying deficiencies in existing laws
- In 2012, Australia ratified the European Cybercrime Convention, adopted a central legislative regime which came into effect in March 2013
- Targets hacking, comp virus propagation and denial of service attacks
- Also includes enhancement of law enforcement powers like search and seizure of electronically stored data
- Strengthens business & community confidence in new technologies by ensuring criminal misuse is penalised

Criminal Code Act 1995

- Section 477 offences are serious hacking offences, whereas 478 offences are not as serious
- Part 10.7, Section 477.1 of the Act:
  A person is guilty of an offence if:
  a) the person causes any unauthorized access, modification or impairment to data held in a computer (hacking) AND
  b) the person knows the access, modification or impairment is unauthorized AND
  c) the person intends to commit, or facilitate the commission of a serious offence against a law of the Cth, a State or Territory (whether by that person or another person) by the access, modification or impairment
  Penalty: life imprisonment or period of more than 5 years
- Section 477.2 of the Act:

  (1) A person is guilty of an offence if:

  (a) the person causes any unauthorised modification of data held in a computer; and
  (b) the person knows the modification is unauthorised; and
  (c) the person is reckless as to whether the modification impairs or will impair:
  (i) access to that or any other data held in any computer; or
  (ii) the reliability, security or operation, of any such data.

  Penalty: 10 years imprisonment.

- Section 478.1 Unauthorised access to, or modification of, restricted data

  (1)A person is guilty of an offence if:
  (a) the person causes any unauthorised access to, or modification of, restricted data; and
  (b) the person intends to cause the access or modification; and
  (c) the person knows that the access or modification is unauthorised.

  Penalty: 2 years imprisonment.

- Issue: Is hacking authorised if you are an employee?
  Hacking within workplace by system administrator → is it unauthorised if they are given the access code as part of their job?

- Section 478.3 Possession or control of data with intent to commit a computer offence
  (1) A person is guilty of an offence if:
  (a) the person has possession or control of data; and
  (b) the person has that possession or control with the intention that the data be used, by the person or another person, in:
  (i) committing an offence against Division 477; or
  (ii) facilitating the commission of such an offence.

  Penalty: 3 years imprisonment.

- Section 478.4 Producing, applying or obtaining data with intent to commit a computer offence

  Penalty: 3 years imprisonment.

<u>Mens rea (fault elements)</u>

- The mental elements: intent, knowledge and recklessness
- In order to establish the mental element of the offences, the summary (ss 478.1 and 478.2) and preparatory offences (ss 478.3 and 478.4) **all require knowledge and intent**
- However, the main offences of unauthorised modification of data (s 477.2) and impairment of electronic communication (s 477.3) **only require recklessness and knowledge**

<u>Recklessness</u>

Defined as being "aware of a substantial risk" and "it was unjustifiable to take that risk" (s 5.4 of Criminal Code)

It is suggested that even a lack of the latest and best anti-viral software may constitute being reckless as to causing impairment because viruses typically cause impairment without authorisation

***Restricted data*** means data:

(a) held in a computer; and
(b) to which access is restricted by an access control system associated with a function of the computer

- It is not a requirement that the data itself is protected by an access control system, only the computer

- Under this definition, the req. of "restricted data" can be easily satisfied because almost all computers/devices are protected by at least a password

Actus reus (physical elements)

The general test is one that requires proof of fault, culpability or blameworthiness both in behavior and mind. Distinguish between:
a) commissions, conduct or positive 'acts'
b) omissions or failures to act

- Access: actus reus of accessing a computer = virtual entrance into the computer by use of a valid username and password

- Authorisation: ambiguities as to what is access without authorization.

The Security Legislation Amendment (Terrorism) Act 2002

Amended the Criminal Code Act 1995 to:
- create a new offence of engaging in a terrorist act and a range of related offences
- modernize Australia's treason offence and,
- create offences relating to membership or other specified links with a terrorist org.

Dishonesty re: carriage services

474.2 – dishonesty with respect to a Carriage Service Provider (CSP):
- anything with the intention of dishonesty obtaining a gain from a CSP by way fo the supply of a carriage service
…
Penalty: 5 years

Interference with telecommunications

474.4 offence to possess, etc an interception device
474.5 offence to cause a communication to be received by a person or CSP other than the person to whom it is directed (except if consent given)
474.6 offence to interfere with facilities

Using network for serious offence

474.14 Similar to Cybercrime Act – offence to connect equipement to the network w intent to commit SO. Specifically includes foreign offences (recognition of juris. Issue)
474.12 An offence to use equipment connected to a telecommunications network in the commission of a SO under Aus/foreign law

Using carriage service to make a threat

474.15 using a carriage service to make a threat (to kill or to cause harm)
474.16 including a false belief (hoax) e.g. bomb threat
474.17 menace, harass or cause offence

Child abuse and pornography

ss 474.19-474.25

Financial information offences s 480.4, 480.5

Evidence

1. Evidence that is relevant in a proceeding is admissible in the proceeding
2. Evidence that is not relevant in the proceeding is not admissible.

Powers granted by the Cybercrime Act

Powers granted to law enforcement. Power to obtain evidentiary material.
Powers of investigation, search and seizure

**COMPUTER CRIME: Case Law**

A. Unauthorised access – system administrator, did he have authority?
Case law on authorised access: (R v Morgan, R v Salter, R v Gilmore)

B. Modification of data to cause harm (also related to financial offences 10.8, existing offences, accomplice)
Case law: (Larkin)

1. Jamie Morgan v Commissioner of Police (2011) NSW

- Section 308H CA: it is an offence to have unauthorised access to or modification of "restricted data" in a computer.
- Facts: Applicant made a series of unauthorised accesses into the COPS database (contains personal, confidential and sensitive info) and failed to properly record or give reason for the access. The applicant improperly released confidential info obtained by the database to Ms Catherine Bell.
- "Restricted data" means data: a) held in a computer, b) to which access is restricted by an access control system.
- Justice Marks found: applicant had not established that his access to the COPS system was authorised "for a purpose consistent with the protocols and procedures established within the NSW police force to secure authorised access".

2. Salter v DPP (2011) NSW

- Section 308H(1): it is an offence where a person knowingly has unauthorised access to restricted data in the computer.
  Section 308B(1): access is unauthorised if the person is not entitled to cause that access

- Facts: The appellant, a police officer, accessed the "COPS" police computer system for **personal reasons**. He was convicted of multiple offences of unauthorised access to restricted data held in a computer under s 308H of the Crimes Act 1900. On appeal, it was submitted that s 308B(2) provides a statutory defence to persons who are authorised to access a computer system but do so for an ulterior motive. The appellant referred to the wording of the provision and to rules of statutory interpretation relevant to construing its meaning.

- The Court of Appeal rejected the submission and dismissed the appeal. McClellan CJ at held that the object of the provision is to protect an officer who has a legitimate entitlement to access particular data, but who may also have an ulterior motive.

3. Gilmour v DPP (1995) NSW

- Take-home message: Hacking within workplace by employee who has access as part of his/her job is still unlawful if he/she commits unauthorised access to, or modification of restricted data.

- Facts: an employee of the ATO was charged with breach of s76C CA. The offender had access via a password and user ID to the Tax office computer. Without the required authorisation from his supervisor, he made entries granting tax-payers relief from obligations.

- NSW Court of Criminal Appeal held: unlawful alteration of data. Although the offender was authorised to use the computer and had the capacity to make the entries, it was not accepted as an answer to the charge for the reason that he had no authority to alter the particular data in question.

4. Larkin v Crown (WA)

- Facts: Larkin and accomplice Shee hacked into Dept of Health in WA and inserted malicious programs. The harmful software was never found, but MSN chat messages showed it had been there at some point. The messages involved Shee suggesting an attempt to hack the computer system of the Dept. of Treasury and Finance. Furthermore in a police interview Larkin indicated that he and Shee had in mind work not just for the Dept of Health but also for other govt. departments. Judge was satisfied that the defendants had acted out personal interests for eventual pecuniary gain.

**INTELLECTUAL PROPERTY**

Property right to information?

There is no general right to property of information

- Covered by statute: patents, copyright, design, trade marks
  Three key elements
  1) they creative negative rights (prevent others from doing something, imposes a duty of forbearance)
  2) they are dependent upon certain criteria being fulfilled
  3) they offer protection for a limited period of time
  Exceptions: trade marks and trade secrets

- *Victoria Racing Park and Recreation Grounds v Taylor*
  Dixon J: the general position is that unless one can bring oneself within some EXISTING form of action or protection, knowledge and information are not the property of an individual.
  The creation of value through the exercise of skill and labour does not *of itself* entitle somebody to a property right in the product of that labour and skill. The exercise of labour and skill has to be brought into some existing category of protection.

- Importance of protection
  There is a significant cost and risk of production. Government schemes in place to encourage innovation
  There is also significant return on investment

Approaches to Protection for IT

- Patents: extensive monopoly on an idea/novel method of manufacture e.g. software
- Copyright: automatic monopoly on public expression of work
- Integrated circuits: specific regime for protecting silicon chips/circuits
- Trade secrets (confidentiality): for IT startup, protection based around confidentiality of info, because there is value in secrets
- Designs: non-functional appearance of a product (shapes and patterns)
- General contract law

Patents

- Governed by the Patents Act 1990
- A patent is a right to commercially exploit a novel/inventive/ useful device/substance/method/process