NATIONAL UNIVERSITY OF SINGAPORE

IFS 4101 – LEGAL ASPECTS OF INFORMATION SECURITY

AY2021/2022, Semester 2, Weeks 6 and 7

THE CRIMINAL JUDICIAL SYSTEM AND COMPUTER CRIMES

REQUIRED READINGS FOR THE TOPIC

1. Teuber, A. (2012). "Defining Crime" in Introduction Phil 22b Spring 2012 [Web log post]. Retrieved 2021, from http://people.brandeis.edu/~teuber/lawintro.html#intro3
2. Interpretation Act 1965 (Singapore) Section 9A.
3. Computer Misuse Act 1993 (Singapore). Compare the 1993, 1998 and the version in effect today.
4. *Singapore Parliamentary Debates, Official Report* (28 May 1993) Vol. 61, Sitting No 3, Columns 300 - 320.
5. *Singapore Parliamentary Debates, Official Report* (30 June 1998) Vol. 69, Sitting No 3, Columns 390 - 420.
6. *Singapore Parliamentary Debates, Official Report* (3 April 2017) Vol. 94 at Second Reading Bills, Computer Misuse and Cybersecurity (Amendment) Bill.
7. Computer Misuse (Composition of Offences) Regulations.
8. *Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin* [1993] 3 SLR(R) 653.
9. *Director of Public Prosecutions v Bignell and Another* [1998] 1 Cr. App. R. 1.
10. *R. v Bow Street Magistrates' Court Ex p. Allison* [2000] 2 A.C. 216.
11. *Lim Siong Khee v Public Prosecutor* [2001] SGHC 69.
12. UK Computer Misuse Act (1990), Sections 1, 2 and 3A.
13. *Public Prosecutor v Law Aik Meng* [2007] 2 SLR(R) 814.

OPTIONAL READINGS FOR THE TOPIC

1. *Public Prosecutor v. Lim Yi Jie* [2019] SGDC 128.
2. *Public Prosecutor v James Raj s/o Arokiasamy* [2015] SGDC 36.
3. *Tan Chye Guan Charles v. Public Prosecutor* [2009] 4 SLR(R) 5.
4. Canada Criminal Law Amendment Act 1985, Section 301.2. See Annex 1.

We will be discussing the topics below in class – either as part of a small group discussion, or you will be called upon to express your ideas about the questions. The topics are based on the readings that you have been assigned to date.

1. WHAT MAKES A CRIME?

Simply put, it is an unlawful act punishable by a state.

But what is it? What are the motivations creating an institution for criminalizing some actions? How do we decide if certain actions should be criminalised (i.e., made a crime that is subject to enforcement through institutional punishment) or not?

HYPOTHETICALS
CASE 1 Peter has a grudge against Vivian. To get back at her, Peter broke into Vivian's house and destroyed her most precious heirloom, the one and only photo of her infant son. He did not have permission to enter her house. Should Peter be punished?
CASE 2 As in Case 1, but Peter and Vivian are employees, Peter accessed Vivian's computer in the office using her password, which she stuck to her monitor using sticky notes, and completely deleted the only electronic copy of her photo from her hard drive. It was well known to everyone in the company that Vivian has made no attempt to hide her password and would regularly tell people to log into her computer using her password to do things on her behalf. Should Peter be punished?
CASE 3 As in Case 2, but Vivian has a back-up copy of the photo in her home computer. Should Peter be punished?
CASE 4 As in Case 2, but Peter was also the company's IT administrator. The company had a policy which did not allow employees to save personal data on office equipment. The policy is 100 pages long and Vivian never read the policy. Peter deleted that photo pursuant to that company policy. Should Peter be punished?

Did you arrive at the same or different conclusion for all the scenarios above? Why? Why not? What are reasons for the different conclusions? Remember the four modalities of regulating behaviour that Lawrence Lessig outlined and apply the modalities language to your analysis.

2. CLASSIFYING ATTACKS AGAINST COMPUTER INFRASTRUCTURE

To have an intelligent conversation about cybercrimes requires us to recognize the different types of attacks that can be made against the computer infrastructure. Some of these cyber activities have their offline counterparts (e.g., fraud), but many are peculiar to the cyber environment. As you try to consider the types of activities that are particular to the cyber world, you may want to answer the following questions:

a) List (as exhaustively as possible) the various forms of cyber-attacks. You may want to indicate your source for your lists.

b) Using a "process-oriented" classification (from preparation to execution), categorize these forms of cyber-attacks.

c) Who carries out these attacks? (Consider insider versus outsider attacks.)

d) What is the rationale for carrying out cyber-attacks? Is it for fiscal gain, the quest for an intellectual challenge or is it something else?

e) Should different punishments be enacted depending on the rationale of the actors? Why or why not?

3. COMPUTER MISUSE ACT 1993 (CMA)

In Singapore, the main piece of legislation defining criminal acts that target the computer system is the Computer Misuse Act, previously known as the Computer Misuse and Cybersecurity Act.

QUESTIONS

1. What is the subject matter of protection under the CMA? Were the Parliamentary Debates helpful in identifying the purpose of the CMA?

2. Does the CMA deal with all the types of cybercrimes that you have identified in response to Section 2 above?

3. Is the CMA meant to cover all criminal activities that take place online? In your opinion, what are the types of cybercrimes that the Act is intended to target?

4. DIFFICULTY OF DEFINITIONS

Review the definition of a computer as given by the CMA. How would you describe the definition? Is it broad enough to cover future technologies? Do you find the various definitions necessary to understanding the legislation and how it should be applied?

In the case of *R. v. McLaughlin*, 113 D.L.R.3d 386, 53 C.C.C.2d 417, 18 C.R.3d 339 (1980), McLaughlin, a student at the University of Alberta, gained access to a university time sharing system without authority. McLaughlin admitted to viewing certain computer files and making some changes to other accounts. He did not commit any other form of economic damage. Given there was no actual taking of any tangible item, it was not possible to convict him under the crime of theft (at that time in Canada, theft was largely tied to the taking of movable property). The only question left, was whether he could have committed a crime under Section 287(2) of the Canadian Criminal Code, which stated:

> *287. (1) Every one commits theft who fraudulently, maliciously, or without colour of right,*
>
> *(a) abstracts, consumes or uses electricity or gas or causes it to be wasted or diverted, or*
> *(b) uses any telecommunication facility or obtains any telecommunication service.*
>
> *(2) In this section and in section 287.1, "telecommunication" means any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by radio, visual, electronic or other electromagnetic system.*

The Supreme Court of Canada held that a computer does not work like a telecommunication facility in that the main function of a computer "is to permit the making of complex calculations, to process and correlate information and to store it, and to enable it to be retrieved," and not to transmit, emit or receive signs, signals, etc. As a result, the conviction against McLaughlin was quashed. Because of this case, Canada rewrote its criminal code to implement Section 301.2 (see Annex 1).

Examine the changes made to the definition of the term "movable property" in Section 22 of the Penal Code (Cap. 224 Rev. Ed. 2008). As a result of the passing of the Criminal Law Reform Act 2019, Section 22 was repealed and replaced with a comprehensive definition of "property" to cover intangible and incorporeal property and virtual currency. This change was enacted to allow the state to punish perpetrators of digital crimes such as criminal breach of trust for misappropriation of virtual currency.

The above examples are given to illustrate the difficulties of drafting criminal provisions that can anticipate future technology and the continued struggles that legislators will have in crafting provisions that keep up with behaviour in cyberspace.

5. THE KNOWLEDGE ELEMENT OF UNAUTHORISED ACCESS

The principal offence in the CMA is the "unauthorised access" offence. Many of the other offences in the CMA are built on or adapted from the "unauthorised access" offence.

To establish the offence of "unauthorized access", Section 3 of the CMA requires a person to "knowingly" cause a computer to perform any function to secure access "without authority".

To understand some of the problems regarding the *mens rea* of the offence, read *Public Prosecutor v Muhammad Nuzaihan bin Kamal Luddin* [1993] 3 SLR(R) 653.

QUESTIONS

1. What are the facts of *Kamal Luddin*? What did the accused do?

2. What was his defence for hacking into SCV's computer system?

3. Did his motive, if at all, alter his mental state?

4. Did the court make hacking a strict liability offence? A strict liability offense is one that is defined solely by the actus reus. The prosecutor is not required to make any investigation into the accused's *mens rea* to determine if a crime has been committed.

5. What is the *mens rea* element of hacking?

6. THE ACTION ELEMENT OF UNAUTHORISED ACCESS

The key action element in Section 3 of the CMA offence is the act of "access[ing] without **authority**". "Access" is defined in Section 2 of the CMA. Subclauses (2) and (5) of Section 2 of the CMA sets out to define the scope of the sub-elements of "access without authority".

QUESTIONS

1. What is the legal definition of "access"? What does "access" comprise?

2. How is the legal definition of "access" different from a technical understanding of what "access" means?

3. How would you interpret the expression "any program or data"? Is it different from a technical definition?

4. How do you interpret the expression "causes a computer to perform any function [to secure] access ... to any program or data held in any computer"? (Which rule(s) of statutory interpretation would you rely on?)

5. Who determines what is "authorised" or "unauthorised" access under the CMA?

Section 3 of the CMA was drafted based on the UK's Computer Misuse Act, so it is instructive to understand how the UK courts interpreted their version of the Computer Misuse Act.

We start with the English Court of Appeal decision in *Director of Public Prosecutions v Bignell and Another* [1998] 1 Cr. App. R. 1. The facts of Bignell were simple. Mr and Mrs. Bignell were both police officers. On six occasions, they instructed computer operators to extract information from the Police National Computer (PNC) for them. They sought this information for private, unofficial purposes. The Police Commissioner had previously ruled that the PNC was to be used for police purposes only, and the Bignells knew this.[1] When their convictions were quashed, the Director of Public Prosecutions ("DPP") appealed by way of case stated to the Divisional Court but without success. The court distinguished the activity of "breaking into computers" from the "misuse of data" . It took the view that the Bignells had indulged in the latter and could not have committed the former because they had the authority to access the data in question.

Two years later, in *R. v Bow Street Magistrates' Court Ex p. Allison* [2000] 2 A.C. 216, the House of Lords was presented with the opportunity to review the *Bignell* decision.

As you read *Ex p. Allison*, ask yourself the following questions:

a) What was the job of the accused? What access did she allegedly make, and for what purpose? Did she have permission to access the data for her intended purpose?

b) What was the ratio of the Ex p. Allison case?

c) How did the House of Lords deal with the Bignell? Would the House of Lords have found the Bignells guilty of accessing the data in question without authority?

Contrast the *Bignell* and *Ex p. Allison* case with *Lim Siong Khee v Public Prosecutor* [2001] SGHC 69.

You will be randomly assigned to a group and should be prepared to identify the *ratio* of *Lim Siong Khee v. PP* and explain any differences in the analyses used by the courts in *Bignell*, *Ex p. Allison* and *Lim Siong Khee*.

7. PHISHING AND UNAUTHORISED PENETRATION TESTING

To understand the Singapore court's treatment of phishing and unauthorised penetration testing, see *Public Prosecutor v. Lim Yi Jie* [2019] SGDC 128 and *Public Prosecutor v James Raj s/o Arokiasamy* [2019] SGDC 36.

[1] Or at least were deemed to be on notice as this matter was stated in a manual which had been issued to them.

8. AGGRAVATED HACKING

To understand Section 4 of the CMA, read Section 2 of the UK CMA and Section 3 of the Singapore CMA.

QUESTIONS

1. How does Section 2 of the UK CMA relate to the offence of "unauthorized hacking"?

2. What is the legislative object behind Section 4 of Singapore's CMA?

3. Is Singapore's Section 4 offence the same as the Section 2 offence under the UK CMA?

4. How does the Singapore's CMA Section 4 offence differ from the same Act's Section 3 offence?

5. Is there a need to maintain Section 4 in the Singapore CMA? Consider your answer in light of *Ex p. Allison* and *Lim Siong Khee*.

Review *PP v Law Aik Meng* [2007] 2 SLR(R) 814 for the application of Section 4 of the CMA. Be prepared to extract and present in class the *ratio* from *Law Aik Meng* decision.

HYPOTHETICALS

CASE 1

Alan (A) hates Vivian (V). He wants to harm her but has no clue where she lives. Without her permission, A accesses V's handphone and got her home address. He proceeds to break into V's house and take her jewellery. Should A be charged under Section 4 of the CMA?

CASE 2

Same as Case 1 except: A was V's HR manager and is authorised to access the HR system. He accessed the HR system to get V's home address. Should A be charged under Section 4 of the CMA?

CASE 3

Same as Case 1 except: A got the HR manager to give him V's home address. A did not know how to get there and, like everyone else, had to get the directions to V's house using Google Maps. Should A be charged under Section 4 of the CMA?

9. UNAUTHORISED MODIFICATIONS

Read Section 5 of the CMA. This is an offense that is independent of Section 3 (contrast Section 4 which is an add-on to Section 3). Understand the statutory definitions of the terms used in Section 5.

QUESTIONS

1. What are the legislative objectives behind Section 5?

2. Which cyber-attack activities were meant to be covered that would not otherwise fall within Section 3 of the CMA?

3. Identify the *actus reus* and *mens rea* elements of Section 5.

4. What is the legal definition of "modification"? What are the elements of the act of "modification"?

5. What is the effect of the "extended causation" clause in the "modification" definition (i.e., the clause that states: "any act which contributes towards causing such a modification shall be regarded as causing it")?

6. How is "modification" similar to "access" in Section 3? How is it different?

7. When is "modification" unauthorised? How do we determine this?

10. UNAUTHORISED INTERCEPTION

Section 6 of the CMA was derived from Section 301.2 of the Canada Criminal Law Amendment Act 1985. Go through the same exercise you just did to understand Section 5 of the CMA.

REAL WORLD SCENARIO

One real world scenario involve the application of Section 6 is the SingTel port scanning incident in 1999. For more information about the incident, see: IMDA, IASPs Get Guidelines on Preventive Security Scanning, 6 January 2000.

1. What were the facts of the case, as reported in the newspapers?

2. What was IMDA's original response to the incident?

3. Why do you think IMDA changed its response to the incident in January 2000?

4. Do you think SingTel's actions were justified? Or do you think SingTel's actions breached Section 6?

11. UNAUTHORISED OBSTRUCTION AND DISCLOSURE OF ACCESS CODES

In 1998, the Computer Misuse Act was substantially expanded with the introduction of two new offences (Sections 7 and 8) and the introduction of a new class of offences (Section 9).

QUESTIONS

1. What are the legislative objectives behind Sections 7 and 8?

2. Which cyber-attack activities were meant to be covered under each of Sections 7 and 8 that were not covered by the CMA before the 1998 revisions?

3. Identify the *actus reus* and *mens rea* elements of Sections 7 and 8.

REAL WORLD SCENARIO

See K. Wong (16 May 2000). *He Swamped HDB with 7,500 Messages*. Straits Times.

1. *What did Tan do? Do you agree that Tan's actions constitute "unauthorized obstruction"? Why? Why not?*

2. *What constitutes "interference" or "impedance"? How could these be proved (or disproved)?*

12. UNAUTHORISED USE OF PERSONAL INFORMATION

In 2017, Parliament enacted new provisions to criminalise the activity associated with the use of "personal information" obtained in breach of the previous provisions of the CMA. See Section 8A and *Singapore Parliamentary Debates, Official Report* (3 April 2017) Vol. 94 at Second Reading Bills, Computer Misuse and Cybersecurity (Amendment) Bill (the "2017 Bill").

QUESTIONS

1. How is Section 8A different from Section 8?

2. Why is it necessary to enact Section 8A?

13. "UNAUTHORISED" ITEMS USED TO COMMIT CYBERSECURITY OFFENCES

In the 2017 Bill, Parliament added a new provision to criminalise the supply or provision of any item which is intended to be used to commit a CMA offence. See Section 10.

QUESTIONS

How does Section 10 distinguish (if at all) between preventive (or defensive) cybersecurity tools such as security check tools and tools that can be used to attack or breach security?

Annex 1

Canada Criminal Law Amendment Act 1985

301.2(1) Every one who, fraudulently and without color of right,

(a) obtains, directly or indirectly, any computer service,

(b) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offense under paragraph (a) or (b) or an offense under 387 in relation to data or a computer system is guilty of an indictable offense and is liable to imprisonment for a term not exceeding ten years, or is guilty of an offense punishable on summary conviction.

(2) In this section, "computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function; "computer service" includes data processing and the storage or retrieval of data;

"computer system" means a device that, or a group of interconnected or related devices one or more of which,

(c) contains computer programs or other data, and
(d) pursuant to computer programs,
    i. performs logic and control, and
    ii. may perform any other function;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system; "electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing; "function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system;

"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.