IFS4101 - LEGAL ASPECTS OF INFORMATION SECURITY

AY2021/2022, SEMESTER 2, WEEK 6

HOMEWORK REVIEW

GENERAL OBSERVATIONS

- **Breach of contract / warranty / guarantee**
  - Seller promised the product will work in a particular manner (will be safe)
  - Product failed to work in that manner (is defective)
  - Damages was caused
- **Fraud**
  - Seller made a representation (e.g., product is safe, it will cure coughs …)
  - That representation is factually wrong
  - Seller knew the representation to be false when seller made the representation
  - Seller intended the buyer to rely on seller's representation to complete the purchase
  - Buyer relied on Seller's representation and was harmed
  - Damages were caused
- **Negligence**
  - Seller owes a duty of care towards the victim
  - Seller failed to carry out that duty
  - As a result of Seller's failure, the victim was harmed
  - The victim's harm resulted in damages for which the court is able to award compensation

ISSUES WITH THE QUESTIONS POSED AND SHORT ANSWERS

- Very generic questions such as: "Is Mixit liable to Brown's mother?"
  - General questions make it difficult to clarify what is the crux of the problem you want to address. Questions should focus on the exactly legal theory that is being asserted to establish liability.
  - Compare a generic question to the following: Does a reseller of goods who did nothing more than to repackage goods that he bought from another manufacturer owes a duty of care to his buyers to ensure the safety of the goods?
- The short answers given were missing the summary analysis. E.g., "Yes, Mixit is liable to Brown's mother."
  - The purpose of the short answer is to help the reader understand quickly the basis for the conclusion reached.
  - A proper short answer is in the form: "Mixit is liable to Brown's mother for negligence because as a reseller, he owed a duty of care to direct and indirect buyers of his products, he breached that duty of care when he failed to conduct safety checks on the product he was reselling, Mr. Brown's mother used his defective product and was harmed, and she incurred medical expenses as a result of that harm.

ISSUES WITH THE ANALYSIS

- The analysis frequently included analysis of theories of liabilities that were not identified as being in play in the "question" section. E.g., the question was about whether or not Mixit was negligent, but the analysis started to talk about breach of product warranty claims.
- Illogical syllogisms. As an example:
  - Premise 1: Mixit did not enter into a contract with Brown.
  - Premise 2: Mixit did not know of the existence of dangerous ingredients in the cough syrup.
  - Conclusion: Therefore, no fraud can be found.
- *Ratios* were copied and pasted from the cases but unclear to me that the student actually understood what the *ratios* meant. Translate the case holdings to plain English for your own benefit.
- Tendency to emphasise quantity over quality. E.g., some students wanted to talk about whether or not Brown can sue on behalf of his son but in the context of answering the question of whether or not Mixit was liable for negligence. **Remember, you get points for coherence, not how many "aha" moments you managed to catch.**

CYBERCRIMES

WHAT IS CYBERCRIME?

- **Wikipedia definition:** Any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.
- **CIA definition:** Crimes that target systems, networks, and data, and seek to compromise their *confidentiality* (i.e., systems, networks, and data are protected and only authorized users can access them), *integrity* (i.e., data is accurate and trustworthy and has not been modified) and *availability* (i.e., data, services, and systems are accessible on demand).
- **Broader Definition:** Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones. – Halderand Jainshankar (2011)

in this case mischief hacking is not really covered here

DIFFERENT LAWS FOR DIFFERENT CYBERCRIMES

- Interaction between the Singapore Penal Code 1871 and Computer Misuse Act 1993
- Singapore Penal Code 1871
  - Targets the acts that constitute crime, whether or not the crime involved was perpetrated using a computer as a tool.
- Computer Misuse Act 1993:
  - Targets actions that involve the use of a computer that constitute a crime.
- **Why is there a need to have a separate statue to regulate activities that may already be criminalised by the Singapore Penal Code 1871?**

HYPOTHETICAL

- Due to COVID-19, Alan has been stuck at home for a few months. He became very bored and spent too much time surfing YouTube. He stumbled onto videos after videos about white hats and decided that he wanted to become one.
- He downloaded some port scanning tools and ran them against some random networks. He discovered network vulnerabilities with Voodoo Company's network. Voodoo makes flying brooms.
- He decided to conduct penetration tests to try to gain access to Voodoo's network. He succeeds after a few tries and managed to get into a folder containing the JPEG files of Voodoo's prototypes of their new flying broom model.
- **Alan uploaded a TXT file containing his name into the folder to prove his success at gaining access.**
- He then sends Voodoo and email to inform them that they need to secure their system and told them to look for the file he inserted into their folder as proof of the visit he paid.

POSSIBLE CRIME(S)?

- **Criminal trespass.** Section 441. Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit "criminal trespass".
- **Mischief.** Section 425. Whoever, with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or any person, causes the destruction of any property, or any such change in any property, or in the situation thereof, as destroys or diminishes its value or utility, or affects it injuriously, commits "mischief".
- **Property.** Section 22.
  - "immovable property" means land, benefits to arise out of land and things attached to the earth or permanently fastened to anything attached to the earth;
  - "movable property" includes property of every description, except immovable property;
  - "property" means money and all other property, movable or immovable, including things in action, other intangible or incorporeal property and virtual currency;
  - "virtual currency" means a digital representation of value in money or money's worth that can be digitally traded and functions as a medium of exchange, a unit of account or store of value, regardless of whether it is legal tender in any country or territory including Singapore.

Alan uploaded a TXT file containing his name into the folder to prove his success at gaining access.

POSSIBLE CRIME(S)?

- **Criminal trespass.** Section 441. Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit "criminal trespass".
- **Mischief.** Section 425. Whoever, with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or any person, causes the destruction of any property, or any such change in any property, or in the situation thereof, as destroys or diminishes its value or utility, or affects it injuriously, commits "mischief".
- **Property.** Section 22.
  - "immovable property" means land, benefits to arise out of land and things attached to the earth or permanently fastened to anything attached to the earth;
  - "movable property" includes property of every description, except immovable property;
  - "property" means money and all other property, movable or immovable, including things in action, other intangible or incorporeal property and virtual currency;
  - "virtual currency" means a digital representation of value in money or money's worth that can be digitally traded and functions as a medium of exchange, a unit of account or store of value, regardless of whether it is legal tender in any country or territory including Singapore.

Alan downloaded one of the JPEG files from Voodoo's folder onto his own computer.

POSSIBLE CRIME(S)?

- **Criminal trespass.** Section 441. Whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit "criminal trespass".
- **Mischief.** Section 425. Whoever, with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or any person, causes the destruction of any property, or any such change in any property, or in the situation thereof, as destroys or diminishes its value or utility, or affects it injuriously, commits "mischief".
- **Property.** Section 22.
  - "immovable property" means land, benefits to arise out of land and things attached to the earth or permanently fastened to anything attached to the earth;
  - "movable property" includes property of every description, except immovable property;
  - "property" means money and all other property, movable or immovable, including things in action, other intangible or incorporeal property and virtual currency;
  - "virtual currency" means a digital representation of value in money or money's worth that can be digitally traded and functions as a medium of exchange, a unit of account or store of value, regardless of whether it is legal tender in any country or territory including Singapore.

Alan inserted some comments into the COM block of one of Voodoo's JPEG files.

Alan uses an editor to edit the binary data of the JPEG file.

Voodoo can easily retrieve a copy of the unadulterated file from its backup.

WHAT TYPES OF ACTIVITIES SHOULD BE CRIMINALISED?

PROCESS-ORIENTED NOMENCLATURE OF CYBERCRIMES

- Preparation
- Input Validation
- Software Tampering
- Authentication
- Authorisation and Configuration
- Communications Management
- Encryption
- Parameter Manipulation
- Data Manipulation
- Exception Management
- Behaviour Manipulation
- Auditing and Logging

PREPARATION

- Vulnerability Scanning
  - Checking targeted system for identification and version information, weaknesses, etc.
- Dumpster Diving
  - Salvaging waste discarded in containers for useful information e.g. passcodes, unerased media
- Pwned Lists
  - Obtaining breached lists of personal data

INPUT VALIDATION

- Buffer-overflow, SQL injection, canonicalization
  - Ways of causing the software to respond in unexpected (but controlled) ways by feeding it "erroneous" or poorly formed input data
- Cross-site scripting (XSS)
  - Injection of client-side scripts into web pages viewed by third parties (stored or reflected)

QUESTIONS

- Which part of the CIA do these attacks target?
- Who carries out these attacks?
- What is the rationale/motive for these attacks?

SOFTWARE TAMPERING

- Virus
  - Malware that replicates by infecting other programs by modifying them
- Worm
  - Standalone malware that replicates itself to spread
- Trojan horse
  - Malicious program used to hack into computer by misleading users of its true intent (hidden part is called payload)
- Backdoor
  - Secret way of bypassing normal authentication
- Zero-day exploit (previously) undisclosed software vulnerability for which there are no defences against exploits

QUESTIONS

- Which part of the CIA do these attacks target?
- Who carries out these attacks?
- What is the rationale/motive for these attacks?

AUTHENTICATION

- Spoofing
  - One person/program masquerades as another by falsifying data
- Man-in-the-middle
  - attacker secretly relays and alters communications between 2 parties who believe they are communicating with each other
- Keylogger
  - software/hardware that covertly records keys struck on keyboard
- Skimming
  - getting private information about somebody’s access card using e.g. a small electronic device to swipe and store victims’ card numbers and passwords

QUESTIONS

- Which part of the CIA do these attacks target?
- Who carries out these attacks?
- What is the rationale/motive for these attacks?

AUTHORISATION

- Privilege escalation
  - process of gaining elevated access to resources normally protected from application or user (by exploiting bug, design flaw or configuration oversight)
- Rootkit
  - software to enable access to computer or areas of software that it would not otherwise be allowed while asking its existence

QUESTIONS

- Which part of the CIA do these attacks target?
- Who carries out these attacks?
- What is the rationale/motive for these attacks?

COMMUNICATIONS MANAGEMENT

- Piggybacking
  - person who tags along authorised person to gain access or entry into restricted resource
- Spyware
  - software that gathers/sends information about person or organization w/o their knowledge/consent

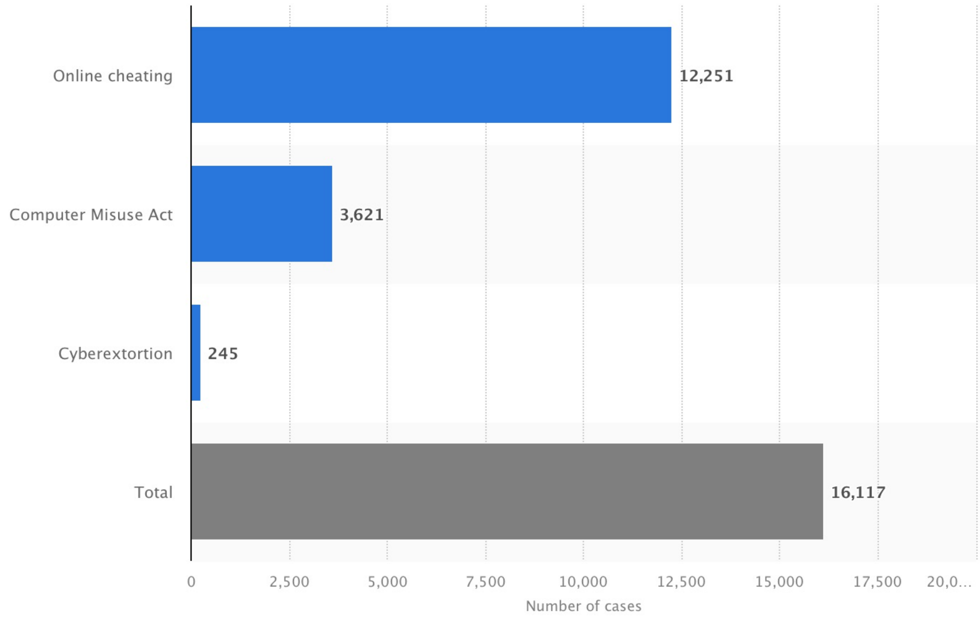
QUESTIONS

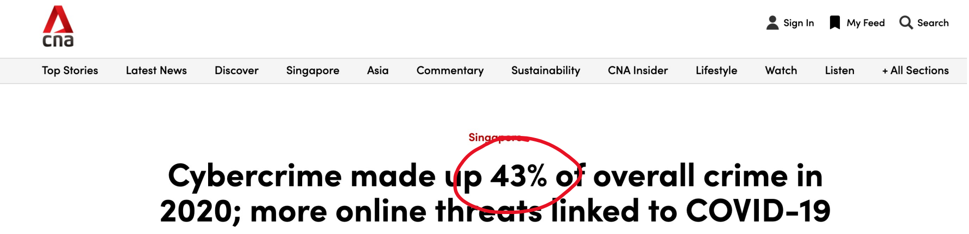
- Which part of the CIA do these attacks target?
- Who carries out these attacks?
- What is the rationale/motive for these attacks?

OTHER FORMS OF CYBER ATTACKS

- Malware
- AdWare
- Ad Fraud
- Ransomware
- Phishing
- Social media and mobile scams
- Online bullying and cyber harassment
- Online cheating

LOCAL CYBERCRIME CASES IN 2020





Cybercrime made up 43% of overall crime in 2020; more online threats linked to COVID-19

LOCAL CYBERCRIME CASES …

- 1998 – 12 months prison for accessing bank computer system to transfer $36,000 into her own account.
- 2003 – 10 months of jail for accessing bank computer system to check if someone was an existing customer of the bank
- 2005 – 21 months jail. ITE student obtained PIN code to a friend's bank account with authorisation initially only to use the PIN code to siphon about $34,00 from four bank accounts.
- 2005 – Man fined $20,000 for asking his Starhub employee friend to access Starhub mobile records to obtain evidence for use in a divorce proceeding. The Starhub employee was also fined $20,000.

LOCAL CYBERCRIME CASES…

- 2005 – NUS 3rd year computer engineering undergrad got friends to install game containing keylogger software, which the student used to unlock Internet banking accounts.
- 2006 – Cybercafe managers used keystroke loggers to capture and steal Diablo users' online treasures worth $15,000. Left off by police with warning.
- 2006 - 17-year-old sentenced to 18 months' probation for illegally "mooching" on an unsecured home wireless network. Probation is typically not offered to people convicted of computer-crime cases as it allows them to have continued access to computers.
- 2014 - The case of "The Messiah" hacker. Charged with 162 computer misuse charges and sentenced to 56 months' jail term. James Raj Arokiasamy, based in Malaysia, exploited reflected XSS vulnerabilities to alter URLs to redirect traffic to new content. Sites attacked included PMO, Straits Times, AMK Town Council, etc.

LOCAL CYBERCRIME CASES…

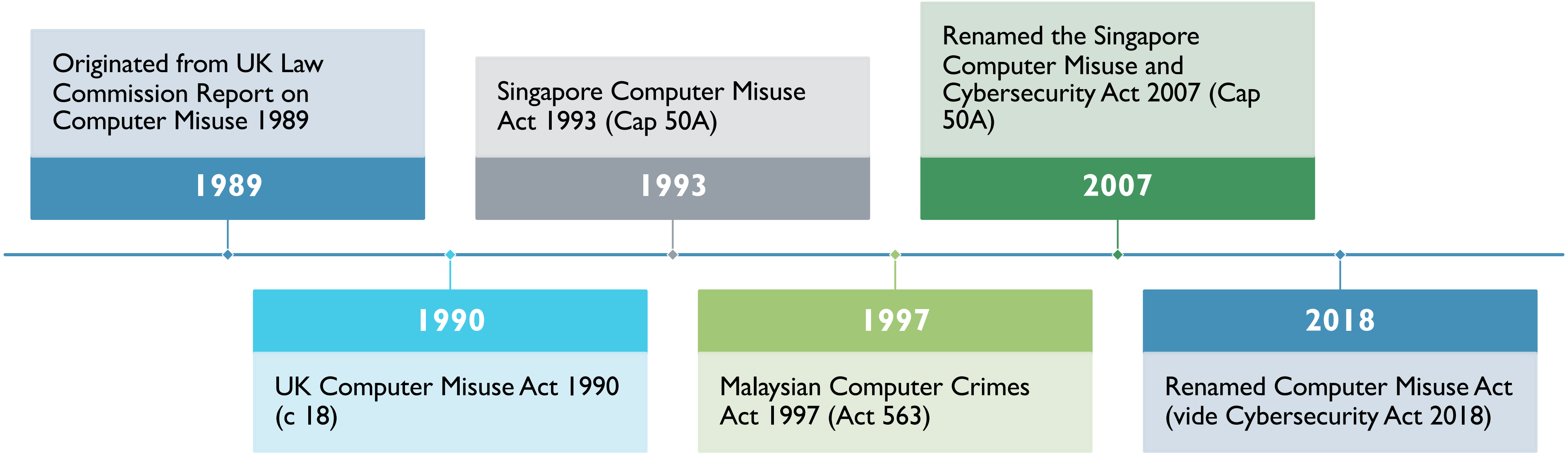
- 2017 – Policeman jailed for one month and eight weeks for using official portal to conduct illegal search on girlfriend.
- 2017 – Man sentenced to three years jail for cheating after buying PayPal and credit card account details on the dark web.
- 2017 – Asean scholar at SMU jailed for 16 weeks for hacking into professor's computer to change grades.
- 2018 – First person charged under Section 8B (now Section 10) of the CMA for obtaining passwords to Facebook accounts and contacting the victims' friends to obtain nude photographs.
- 2018 – Parking officer sentenced to four weeks' jail for issuing summons to motorists who had not broken any rules by entering registration numbers of vehicles without season parking tickets into an electronic database.

LOCAL CYBERCRIME CASES…

- 2019 – Two weeks' jail for man who changed his records so that he could be permanently exempted from the Individual Physical Proficiency Test (National Service requirement).
- 2019 – 13 years' jail for banker for cheating more than $13.6 million from bank clients.
- 2020 – NTU student convicted for hacking Kopitiam stored value cards.
- 2021 – Contract consultant implemented a backdoor while implementing a power monitoring control system for MBS through which he caused a blackout at the casino.
- 2021 – Woman charged for unauthorised access under the CMA for disclosing over 1,100 bank customer information to scammers
- 2021 – 10 arrested and charged under the CMA for fraudulently registering pre-paid SIM cards

THE COMPUTER MISUSE ACT 1993

BACKGROUND



1989

Originated from UK Law Commission Report on Computer Misuse 1989

1990

UK Computer Misuse Act 1990 (c 18)

1993

Singapore Computer Misuse Act 1993 (Cap 50A)

1997

Malaysian Computer Crimes Act 1997 (Act 563)

2007

Renamed the Singapore Computer Misuse and Cybersecurity Act 2007 (Cap 50A)

2018

Renamed Computer Misuse Act (vide Cybersecurity Act 2018)

HOW TO READ SINGAPORE'S LAWS

- Where to find it:
  - http://statutes.agc.gov.sg (free, primary legislation only)
  - http://www.lawnet.com.sg (subscription, primary + secondary legislation)
  - http://libproxy1.nus.edu.sg/login?url=http://www.lawnet.sg/lawnet/ip-access (NUSLibrary subscription)
- How to read it:
  - Short Title (which will indicate the year of original enactment)
  - Long Title
  - Chapter Number (in older references)
  - Year of revised edition
  - Date of version
  - Interpretation
  - Sections
  - Bill and Explanatory Statement

COMPUTER MISUSE ACT 1993

- Long Title
  - "An Act to make provision for securing computer material against unauthorised access or modification and for matters related thereto."
- What subject matter comes under the scope of the CMA?
- Does the CMA deal with all types of cybercrimes?

COMPUTER MISUSE

SECTION NO.	SUBJECT MATTER
3	Unauthorised access to computer material
4	Access with intent to commit or facilitate commission of offence
5	Unauthorised modification of computer material
6	Unauthorised use or interception of computer service
7	Unauthorised obstruction of use of computer
8	Unauthorised disclosure of access code
9	Supplying, etc., personal information obtained in contravention of certain provisions
10	Obtaining, etc., items for use in certain offences
11	Enhanced punishment for offences involving protected computers
12	Abetments and attempts punishable as offences

HACKING / UNAUTHORISED ACCESS

THE CRIME OF UNAUTHORISED ACCESS UNDER S 3, CMA

Unauthorised access to computer material.

> ***3.***--*(1) Subject to subsection (2), any person who <u>knowingly causes</u> a computer to <u>perform any function</u> for the <u>purpose of securing access without authority</u> to any <u>program or data held in any computer</u> shall be guilty of an offence and shall be liable on conviction –*
>
> *(a) to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both; and*
>
> *(b) in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.*

(CON'T)

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at —

(a) any particular program or data;
(b) a program or data of any kind; or
(c) a program or data held in any particular computer.

this part is the understanding where some crime committed cause damage, as compared to mischievous acts

WHAT ARE THE ELEMENTS OF THE CRIME OF UNAUTHORISED ACCESS UNDER SECTION 3(1)?

"*any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer*"

- (1) a person must (2) knowingly cause (3) a first computer to (4) perform any function to (5) [function must] secure access (6) to any program or data held (7) in any computer (including a computer that is different than the first computer).

What does "knowingly cause" mean?

Option 1	**Option 2**
Knowingly caused a computer to perform the function AND Access to the program or data is secured without authority BUT The person is not aware that access is unauthorised	Knowingly caused a computer to perform the function AND Person knows that the access has been secured without authority

WHAT DOES THE TERM "KNOWINGLY" MEAN IN S 3, CMA?

To understand what the term "knowingly" means we turn to *PP v Muhammad Nuzaihan bin Kamal Luddin* [1999] 3SLR(R) 653.

- What were the facts of the case?
- What was the defendant's defence?
- Did the defendant's motive alter his mental state?
- According to Yong CJ, is the crime of unauthorised access to computer material meant to be a strict liability offence? Strict liability means no *mens rea* is required.
- What is the *mens rea* of "unauthorised access"?

BACKGROUND OF *PP V. KAMAL LUDDIN*

- In July 1998, the accused (A) hacked into two Linux-based systems.
- He secured system administrator privileges (root access) on Swiftech Automation's server called Cloud4. Swiftech operates a proxy server and is a Value-added Service Provider for SingNet.   A downloaded 'ROTShB' (Riders of the Short Bus) exploit onto Cloud4.
- A operated an Internet Relay Chat service on the Cloud4 server by uploading the program 'bounce' for his second hack to reconfigure port 31337 of the Cloud4 server to create an IRC account for himself. A then boasted about his exploits on IRC
- A also secured system administrator privileges on SCV's server, Brahms, and modified the contents of the file 'inetd.conf' and configured a backdoor ('nightman') at port 22 to allow him future access.
- A deleted system logs before logging out to cover his trails.
- A claimed that he not commit the offences out of greed nor did he at any time harbour any evil or sinister intent. He was not a gang member and the offence in question was not violent in nature.
- District judge held that A was merely checking for vulnerabilities in computer networks. Sentenced to 30 months probation.
- Prosecution appealed

THE KAMAL LUDDIN DECISION BY CJ YONG

- Ruling, on appeal, by CJ Yong Pung How:
  - Sentence was **manifestly inadequate** and that the inherent nature of the offences under the CMA made **probation orders ineffective**.
  - Imposed 6 months jail
- "19. ... [Describing accused's hacking activities as being motivated by dissatisfaction with SCV's responses] A teenager ... who commits such offences must be intelligent enough to know that it is wrong and dishonest of him to do so and the punishment for these offences must be brought home to him directly ... As a result, when offences such as these are committed, the courts **may well have to apply the principles of strict liability** so that the offender's state of mind is irrelevant to a finding of guilt."

(CON'T) THE KAMAL LUDDIN DECISION BY CJ YONG

- "Checking/probing system for vulnerabilities is still 'hacking' "
- "21. ... In my view, such anti-social conduct on the part of the respondent not only undermines public and international confidence in the commercial integrity and viability of our computer systems, it also gravely compromises Singapore's efforts to position itself as a global e-commerce hub. The potential for which these cyber-crimes have in undermining Singapore's burgeoning information technology (IT) industry cannot be ignored. IT security is a major consideration which many foreign companies take into account before deciding whether or not to develop and invest in the local IT sector."

(CON'T) THE KAMAL LUDDIN DECISION BY CJ YONG

- "…. In particular, during the second reading of the Computer Misuse (Amendment) Bill on 30 June 1998, the Minister noted at column 392 that:
  - *… crimes committed through the electronic medium and through use of computers are difficult to detect but they are just as serious as traditional crimes and we must equally protect our population against such crimes. To **ensure that Singapore remains an attractive place for investors and businesses to operate effectively and securely**, computer crimes must be treated **as seriously as other criminal offences**.*
- In the result, I had no hesitation that a deterrent sentence had to be meted out on the respondent in order to give effect to Parliament's express intention that all computer crimes will be dealt with severely in Singapore."

WHAT IS THE MENS REA REQUIRED UNDER S 3, CMA?

- What is the requisite mental state for hacking?
  - Is CJ Yong's statement in paragraph 19 the *ratio* or *obiter* of the case?
  - Did the facts of the case suggest that the accused knew that his access into the system would be unauthorised? Was his claim that he was merely "checking for vulnerabilities" valid?
  - How do we determine his statement of mind? By his own testimony or an objective test?
    - Objective test of knowledge (Cf. *Bridges Christopher* [1998] 1 SLR 162 (CA)
- Is section 3 of the CMA a strict liability offence?
  - Strict liability offences are "faultless" offences – intention, knowledge, negligence are all irrelevant.
  - No.

COMPARING S 3 OF SINGAPORE'S CMA WITH S 1,OF THE UK CMA

- **SINGAPORE COMPUTER MISUSE ACT 1993**
- **Unauthorised access to computer material.**
- **3**-- *(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction …*

- **UNITED KINGDOM COMPUTER MISUSE ACT 1990 (c 18)**
- **Unauthorised access to computer material.**
- *1--(1) A person is guilty of an offence if--*

  (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secured;

  (b) the access he intends to secure, or to enable to be secured, is unauthorised; and

  (c) he knows at the time when he causes the computer to perform the function that that is the case.

WHAT DOES "ACCESS" MEAN?

WHAT DOES THE TERM "ACCESS" MEAN IN S 3, CMA?

- What is the legal definition of "access"? See Section 2(2).
- Is the legal definition different from a technical definition of "access"? What about from an English definition of access"
- Is there anything that could be "access" from a technical understanding that is not "access" according to the legal definition?
- 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?)

THE DEFINITION OF THE TERM “ACCESS” IN THE CMA

Interpretation

2 - (2) *For the purposes of this Act, a person secures* ***<u>access</u>*** *to any program or data held in a computer if by causing a computer to perform any function he --*

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner),

and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.

(CON'T) THE DEFINITION OF THE TERM "ACCESS" IN THE CMA

(3) For the purposes of subsection (2)(c), a person uses a program if the function the person causes the computer to perform —

(a) causes the program to be executed; or

(b) is itself a function of the program.

(4) For the purposes of subsection (2)(d), the form in which any program or data is output (and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

WHEN IS ACCESS UNAUTHORISED UNDER THE CMA?

2-- *(5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if the person —*

(a) is not himself or herself <u>entitled to control access</u> of the kind in question to the program or data<u>; and</u>

(b) <u>does not have consent</u> to access by him or her of the kind in question to the program or data from any person who is so entitled.

WHO HAS AUTHORISED ACCESS UNDER S 3, CMA?

- Someone entitled to control access can never be charged with the offence of hacking
  - Systems operator? IT manager?
- What if accounts are shared?
  - E.g. CEO getting his secretary to check his email
- What if permission was granted and subsequently withdrawn?
- What if authorised access is made for an unauthorised purpose?

there must be both:
- technological boundaries
- written policies (contractual safeguards)

to properly determine what kind of access is authorised

UNAUTHORISED ACCESS REQUIRES TWO QUESTIONS TO BE ANSWERED

- Q1. What objects must be "accessed"?
- Q2. Who determines what is "authorised" access?

UK UNAUTHORISED ACCESS – "ACCESS"
DPP V BIGNELL [1998] 1 CR. APP. R. 1

- A1 and A2 were police officers serving with the London Metropolitan Police
- A1 left his wife W to live with A2
- W started to see somebody, who parked one of two cars at W's place
- Between December 1994 and May 1995, A1 and A2 instructed police computer operators of the Police National Computer to extract information regarding the registration and ownership details of the two cars
- A1 and A2 traced the cars to one H, W's new partner

UK UNAUTHORISED ACCESS – "ACCESS"
DPP V BIGNELL [1998] 1 CR. APP. R. 1

- Both A1 and A2 were deemed to be aware of the following directions from the Police Commissioner:

  "All information on the PNC2 (Police National Computer) is confidential and is for POLICE USE ONLY. Access to all police data is permitted only for the purposes necessary for the efficient discharge of genuine police duties in accordance with Service policies and procedures. Personal or private use of PNC2 is strictly forbidden."

- Lower court judgment:
  - A1 and A2 as police officers were authorised to access the Police National Computer system
  - But they were authorised to do so for official, police purposes
  - They were not permitted to use information accessed for non-police (private) purposes

UK UNAUTHORISED ACCESS – "ACCESS"
DPP V BIGNELL [1998] 1 CR. APP. R. 1

- At the appellate level, their convictions were quashed
- The reason given was:
  - A1 and A2 had authority to access, even though access was for an unauthorised purpose
  - Primary purpose of the UK CMA was to safeguard against hacking – i.e., *integrity of information* contained in computers, not the purpose to which information is used

UK UNAUTHORISED ACCESS REVISITED

R V BOW STREET MAGISTRATES COURT EX P. ALLISON [2000] A.C. 216

- A worked for American Express and had access to AMEX’s computer system
- A was authorised to access computer records of those who owed money to AMEX
- A was instructed by AMEX to only access those accounts she was working on, and not to access the other accounts, even though she had the ability to access all the accounts
- A accessed the other accounts, obtained account information and passed it on to A2 and A3 who made forged AMEX credit cards and obtained large sums of money
- A was charged with securing unauthorised access to data (accounts) on the AMEX computer.

(CON'T) UK UNAUTHORISED ACCESS REVISITED
R V BOW STREET MAGISTRATES COURT EX P. ALLISON [2000] A.C. 216

Held:

- "unauthorised access" meant unauthorised "access to the data", and not merely unauthorised "access to the computer [which houses the data]".
- (at 10) "... [T]he term 'hacking' is used conveniently to refer to all forms of unauthorised access whether by insiders or outsiders and that the problem of misuse by insiders is as serious as that by outsiders ... An employee should only be guilty of an offence if his employer has clearly defined the limits of the employee's authority to access a program or data."

unauthorised access is really technical and clear - if a policy stated the exact boundaries which someone is authorised to access - then anything outside of that policy is unauthorised - even if they had the credentials to access those other sections

WHAT HAPPENED? WHY DID THE COURT SWITCH?

- What were the relevant facts of the Allison Court? Did the accused have permission to access the data for her intended purpose?
- What was the *ratio* of the case?
- Would the House of Lords have found the accused in Bignell guilty? Why? Why not?
- Does the Allison decision apply to a private setting? Keep this in mind for the discussion concerning *Lim Siong Khee.*

GROUP DISCUSSION TIME

- How does the decision in *Lim Siong Khee v PP* [2001] SGHC 69 differ from Allison or Bignell?

KEY THINGS TO NOTE ABOUT UNAUTHORISED ACCESS CASES

- "Unauthorised access" is *not* a strict liability offence – "knowledge" must be proven
- Broad definition of "access"
  - Very few activities will *not* be caught by legal definition of "access"
- How to determine when access is unauthorised?
  - Authority to access is determined by companies through their policies
  - Authority to access is determined by contractual terms and policies set out on websites and general industry practice
  - Authority access is granted by the owner of the data
  - How can one make it clear that access is "unauthorised"?
  - What are the possible issues with the legal concept of "authorised access"?

when it comes to the purpose - depends on the policy

ACCESS WITH INTENT TO COMMIT OFFENSE

CMA S 4 : ACCESS WITH INTENT TO COMMIT OFFENSE

Access with intent to commit or facilitate commission of offence

4. *---(1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.*

(2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

(3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(4) For the purposes of this section, it is immaterial whether —

(a) the access referred to in subsection (1) is authorised or unauthorised;

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.

INTRODUCED BY 1998 AMENDMENTS TO S 4 OF THE CMA

- "unauthorised" access: s 3 *plus* **intent** to commit an offence (motive / *mens rea*) involving property, fraud, dishonesty and causes bodily harm
- Explanatory Statement (1993)
  - Clause 4 creates an offence of committing the unauthorised access offence under clause 3 with intent to commit or facilitate the commission of a further, more serious, offence.
- Explanatory Statement (1998)
  - Clause 4 repeals and re-enacts section 4 to make it an offence to gain access for the purpose of facilitating or committing certain other offences. Authorisation of access is immaterial.
- Enhanced punishments
  - $50k or10 years imprisonment or both
- It is **immaterial** whether
  - Access is **authorised or unauthorised**
  - Offence committed at same time as securing access

SECTION 4 CMA ILLUSTRATIONS

- A1 takes advantage of the "buffer-overflow" exploit in Microsoft software to give himself administrator privileges on an unpatched server belonging to a bank
  - S 3(1) offence – unauthorised access
- Next, A1 manipulates the bank accounts on the server to transfer funds from third parties into his own account
  - S 4(1) offence – unauthorised access to system with intent to commit a further offence of theft of funds
- A2, the system's administrator for the bank, manipulates bank accounts and transfers funds into his own account
  - S 4(1) offence – access may be authorised, but access was with intent to commit a further offence of theft of funds

COMPARE S4 CMA TO UK CMA S2

Singapore CMA

Access with intent to commit or facilitate commission of offence

4. ---(1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.

(2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

…

(4) For the purposes of this section, it is immaterial whether —

(a) the access referred to in subsection (1) is authorised or unauthorised;

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.

UK CMA

2 Unauthorised access with intent to commit or facilitate commission of further offences.

(1)A person is guilty of an offence under this section if he commits an offence under section 1 above (“the unauthorised access offence”) with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2)This section applies to offences—

(a) for which the sentence is fixed by law; or

(b) for which a person who [is no longer a minor] and has no previous convictions may be sentenced to imprisonment for a term of five years [..].

MID-TERM

TOPICS FOR MID-TERM

- Weeks 1 through 6
- Closed book
- TBD but likely a combination of MCQ, short questions and one long open-ended question