

Computer Law and Investigation

ST2502

Assignment: CA2 Report

Class: DISM/FT/1B/04

|  |  |
| --- | --- |
| **Student Number** | **Full Name** |
| 1928864 | Lu Jia Jun |
| 1904291 | Chye Mun Kiat, Sean |
| 1904189 | Lee Yi Terng |
| 1950065 | Haziq bin Affendy |
| 1904361 | Lee Kah Boon |

Submitted to: Mrs Adeline Lee

Date: 6 February 2020

# Executive Summary

Computer crimes are incredibly prevalent in today’s world. It is of utmost importance to ensure that there are laws and measures properly implemented in order to deter these crimes from being committed.

This report is increasingly relevant as computers and mobile devices become more widely used in society today for our daily tasks. This report details the applications of the Computer Misuse Act and other relevant laws to prevent and prosecute such crimes involving computers and possible breach of privacy.

This report contains a background introduction to the Computer Misuse Act, examples of the Computer Misuse Act being used to prosecute computer criminals, various practical measures that can be undertaken to prevent computer crimes, as well as discussing the applications of the Personal Data Protection Act.

Table of Contents

[Executive Summary 2](#_Toc31834966)

[1. Introduction 5](#_Toc31834967)

[2. Computer Misuse Act 5](#_Toc31834968)

[2.1 Introduction 5](#_Toc31834969)

[2.2 Background 5](#_Toc31834970)

[2.3 Objectives 6](#_Toc31834971)

[2.4 Mitigating Factors 6](#_Toc31834972)

[2.5 Part 1 of the Statute 6](#_Toc31834973)

[2.6 Part 2 of the Statute 6](#_Toc31834974)

[2.7 Part 3 of the Statute 7](#_Toc31834975)

[3. Practical Measures 7](#_Toc31834976)

[3.1 Practical Measures overview 7](#_Toc31834977)

[3.2 Passwords 8](#_Toc31834978)

[3.3 Updating Systems 8](#_Toc31834979)

[3.4 Identity 8](#_Toc31834980)

[3.5 Mobile Phones 9](#_Toc31834981)

[4. How can the Computer Misuse Act be used to prosecute computer criminals? 9](#_Toc31834982)

[4.1 Computer Misuse Act 9](#_Toc31834983)

[4.1 Red Cross Website Hacked 9](#_Toc31834984)

[4.1 PP v Ricky Widjaja (2015) 10](#_Toc31834985)

[4.2 PP v Koh Chee Tong (2016) 10](#_Toc31834986)

[4.3 Muhammad Nuzaihan vs PP (1999) 10](#_Toc31834987)

[5. Discussing the Issue of Privacy of Individuals 11](#_Toc31834988)

[5.1 The Beginning 11](#_Toc31834989)

[5.2 The Ideal 11](#_Toc31834990)

[5.3 The Consequences 11](#_Toc31834991)

[5.4 An Example 12](#_Toc31834992)

[6. Can privacy be resolved under the provisions of the Personal Data Protection Act/law of confidential information? 12](#_Toc31834993)

[6.1 Consents: 12](#_Toc31834994)

[6.2 Purpose: 12](#_Toc31834995)

[6.3 Reasonableness: 13](#_Toc31834996)

[7. Conclusion 13](#_Toc31834997)

# 1. Introduction

Computer crimes are becoming a huge problem in our society today. With the increased use of computers and mobile devices in our daily lives, the threat that computers pose to us is also becoming greater. Computer crimes are real-world crimes that are perpetrated using a computer. Cyber and computer crimes now account for close to a staggering one-fifth of all crimes committed in Singapore.

To counter this onslaught of computer crimes, Singapore has put in place multiple laws such as the Computer Misuse Act, the Cybersecurity Act, the Personal Data Protection Act, and many more. Laws aside, there are also many codes of ethics drafted by companies such as the Infocomm Media Development Authority.

These laws are crucial as they provide a way to punish and retribution for committing the offence of computer crime by issuing fines and a jail term. These penalties will deter potential cybercriminals from wanting to commit these crimes.

# 2. Computer Misuse Act

## 2.1 Introduction

The Computer Misuse Act was first enacted in 1992 and last amended in 2017. It was originally created to address computer crimes in Singapore and to take a more sophisticated approach to provide for enhanced penalties proportionate to the different levels of potential and actual harm caused by computer crimes. It is currently Singapore’s principal legislative response to computer crime.

Computer crime is defined as:

“An act that is performed by a knowledgeable computer user sometimes referred to as a hacker that illegally browses or steals a company’s or individual’s private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.”(Definitions and Hope, 2020)

## 2.2 Background

The need for a Computer Misuse Act came about as Information Technology has become very pervasive in every aspect of society such as the government and business industries.

There were 6179 cybercrimes in 2018, up from 5351 in 2017. This shows that there is a rising crime rate related to the use of computers and further emphasizes the need for the Computer Misuse Act.

## 2.3 Objectives

The Computer Misuse Act was developed to enhance security in areas like bank transfers, defence, telecommunication, public utilities and many other critical infrastructures. It carries out punishment to commensurate the severity of the offence.

## 2.4 Mitigating Factors

If someone is caught breaching the laws laid out in the Computer Misuse Act, there are various pieces of information or evidence about the defendant and circumstances of the crime that might result in reduced charges or a lesser sentence.

Good mitigation factors include “First Offence” submissions, Plea of Guilt at the earliest opportunity and many more.

Poor mitigation factors include Ignorance of the law, “Sole BreadWinner” theory and intoxication.

## 2.5 Part 1 of the Statute

Part 1 of the statute states the short title and gives definitions of what certain terms mean. For example, Section 2 states that “computer” means an electronic, magnetic, optical, electrochemical, data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such devices or group of such interconnected or related devices.

## 2.6 Part 2 of the Statute

Part 2 of the statute comprises Section 3 to 10 regarding the offences of the Computer Misuse Act. This Section states the offence, what action constitutes committing the offence, as well as what punishment will be the result of committing the offence. This part contains information on hacking, modification of computer contents, email bombing, protected computers and many more.

For example, in Section 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 to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, 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.

An overview of the Sections under Part 2 of the Statute:

Section 3 - Unauthorized Access to Computer Material

Section 4 - Access with intent to commit or facilitate the commission of the offence

Section 5 - Unauthorized modification of computer material

Section 6 - Unauthorized use or interception of computer service

Section 7 - Unauthorized obstruction of use of computer

Section 8 - Unauthorized disclosure of access code

Section 8A - Supplying personal information obtained in contravention of certain provisions

Section 8B - Obtaining items for use in certain offences

Section 9 - Enhanced punishment for offences involving protected computers

Section 10 - Abetments and attempts punishable as an offence

## 2.7 Part 3 of the Statute

Part 3 of the Computer Misuse Act comprises Section 11 to 16, with Section 15 and Section 15A repealed as of 2005 and 2018 respectively. This part discusses the Miscellaneous and General aspects of the Computer Misuse Act. The Sections in this Part contain information such as the Territorial scope of offences under this Act, the Amalgamation of charges, the jurisdiction of courts to hear and determine all offences under this Act, allow police officers to arrest without warrant when a person is reasonably suspected of committing an offence under this Act and many more.

An overview of the Sections under Part 3 of the Statute:

Section 11 - Territorial scope of offences under this Act

Section 11A - Amalgamation of Charges

Section 12A - Composition of Offences

Section 13 - Order of payment of compensation

Section 14 - Saving for Investigations by police and law enforcement officers

Section 15/15A - Power of police officer to access computer and data (Repealed)

Section 16 - Arrest by police without a warrant

# 3. Practical Measures

## 3.1 Practical Measures overview

Computer crimes are usually consequences of human negligence. For example, negligence of installing computer upgrades, negligence of cybersecurity training for employees and many more.

Practical measures are preventive actions that can be implemented to reduce the risk of being hit by computer crimes. Some examples of preventive measures include: Protecting systems with strong passwords, keeping computer systems up-to-date and protecting your identity online.

## 3.2 Passwords

Protecting systems with a strong password is very easy to implement. By using a strong and unique password, it is arduous for hackers to crack it. Passwords should not include any personal information, which includes identification numbers and birth dates. They should be at least 16 characters in length with a combination of upper and lowercase alphanumeric characters and symbols. “As we’ve seen, eight-character passwords give you over 221 trillion combinations, which can be reasonably brute-force guessed offline in hours.

Twelve characters gives you over three sextillion (3,279,156,381,453,603,096,810). The offline brute-force guessing time, in this case, would be measured in *centuries*. Sixteen takes the calculation off the chart. That’s why 16 is better than 12, and both are better than eight.”(Larson et al., 2020) It is not advisable to use the same passwords for multiple sites or systems as it will increase the risk of detection and might lead to password exploitation. Moreover, do not write down passwords and leave it in close vicinity of the system it was intended for. Passwords should be changed regularly, most preferably 3 months, as they are locks that lead others to your own personal information.

## 3.3 Updating Systems

Keeping computer systems updated is extremely vital as vulnerability and exploits of older and legacy systems are regularly found and posted on websites such as <https://cve.mitre.org/> and [www.cvedetails.com](http://www.cvedetails.com) . It is very simple to update a pre-existing system that is not too old. For example, on the Windows operating system service packs and feature packs upon release will come with a notice and a summary of the update fixes. These service packs are very important as they patch up specific vulnerabilities, therefore preventing potential attackers from using that as an exploit into a system.

## 3.4 Identity

You yourself determine your identity online. An impersonator can pretend to be you and cause mayhem online, anything that he/she has done will be directly tied to you as technically he/she is identified as you. This is called identity theft. Identity theft is serious as it can easily be used to spread false information while posing as a reputable individual. This can be avoided by following a few simple steps: “It is critical that you be cautious when giving out personal ID such as your name, address, phone number and/or financial information on the internet. Be certain to make sure that websites are secure when making online purchases or entering personal identification. This can also include enabling your privacy settings when using social networking sites.”(Bandakkanavar, 2020)

## 3.5 Mobile Phones

Additional steps may include securing one’s personal mobile phone. Our mobile phones contain all our own notes and credentials. The contents in a phone can be backed into another remote location such as a cloud or a server. Therefore, anything that is stored in any device has a backup copy. To reduce the risk of hackers gaining access to information, there are a few measures that can be taken. First, Mobile phones can be encrypted to prevent hackers from getting to the information unless they have the key to decrypt it. Secondly, refrain from entering personal credentials into one’s own personal mobile phone. Anyone with access to the phone will have access to the credentials. Lastly, one of the easiest ways to protect one’s phone is to lock the phone. By denying access to the mobile phone, it requires the hacker to put in more effort to break into the phone.

# 4. How can the Computer Misuse Act be used to prosecute computer criminals?

## 4.1 Computer Misuse Act

The Computer Misuse Act (CMA) created 10 sections from 3 to 10 to explain the different types of computer crime. These sections help the authority to identify what type of computer crimes has been committed and to administer the correct punishment. Without the Computer Misuse Act, it would be impossible to differentiate computer crimes.

## 4.1 Red Cross Website Hacked

On May 8, 2019, The Singapore Red Cross website, a humanitarian organization, was hacked which resulted in compromising the personal data of more than 4,200 people, including their full names, contact numbers and email addresses.

This Incident was a violation of section 3 of the Computer Misuse Act, unauthorized access to computer material. The perpetrator although was not caught would be liable to a fine up to $50,000 or imprisonment up to 7 years as this incident causes damage to people's lives

The perpetrator did not only violate the Computer Misuse Act but also the Personal Data Protection Act. He or she would also be liable to whatever punishment the Personal Data Protection Commission decides.

## 4.1 PP v Ricky Widjaja (2015)

An example of the CMA prosecuting criminals would be the **PP v Ricky Widjaja (2015)** case. The accused, Ricky Widjaja a former sports betting trader who cheated Singapore Pools pleaded guilty to 13 charges under section 4(3), accessing a computer with intent to commit an offence, section 10(1) abetting with another person, Thomas Tong Heng Huat, to commit an offence. He was sentenced to 4 years in jail.

## 4.2 PP v Koh Chee Tong (2016)

Another example for the CMA in action is the **PP v Koh Chee Tong (2016)** case. In this case, the accused Koh Chee Tong was a compliance officer within the United Overseas Bank who had a loan shark debt. He used his position in UOB to obtain names of several account holders in order to lighten his debts. Under the CMA he had performed an offence under section 3, he was charged with 4 counts of unauthorised access to data in the computer system of UOB under section 3(1) of the CMA and was sentenced to 24 weeks of jail.

## 4.3 Muhammad Nuzaihan vs PP (1999)

The last example is the **Muhammad Nuzaihan v PP (1999)** In this case the accused was a 17-year-old student who had committed crimes under section 3,5 and 6 of the CMA. The act was, he gained unauthorized access into the computer files in Swiftech network, he executed a program to allow him to gain access to a computer service in order to create an account for himself and he gained unauthorized access to the Singapore Cable Vision so that he may have internet access. He was sentenced to 6 months of imprisonment.

As can be seen from the three examples the Computer Misuse Act is effective at prosecuting computer criminals. Thanks to the Computer Misuse Act the authorities were able to identify the different computer crimes that were committed and charge the criminals to the fullest extent.

To conclude, the Computer Misuse Act can help prosecute cyber criminals by setting a standard guideline to cases revolving around computer crimes. This standard guideline will be very useful in creating new laws in the future. Using the CMA, the severity of the crime is easily classified and the appropriate punishment(s) can be carried out without complications.

# 5. Discussing the Issue of Privacy of Individuals

## 5.1 The Beginning

Back in 2014, Prime Minister Lee Hsien Loong made clear the government’s plans for Singaporeans - the plan to transform Singapore into a “Smart Nation”, implementing new schemes to shift people’s lives onto technological platforms. For example, the current Electronic Road Pricing (ERP) system will be replaced by a new, satellite-based one which charges motorists based on distance spent on designated roads. Many had concerns about this proposed islandwide digitisation, especially on how far its policies would infringe on the privacy of Singaporeans.

## 5.2 The Ideal

Theoretically, a “Smart Nation” should maximise *both* efficiency and data privacy, but the actual “Smart Nation” that Singaporeans are living in is one where personal data is widely collected, inadequately protected, and easily misused. Furthermore, criticisms of Singapore’s flimsy data protection regime are valid but insufficient. There are deeper issues which must be fixed for real progress to be possible, including a ruling elite that benefits from keeping the public in a state of ignorance and apathy.

Some might say that they don’t have a problem with the rapid consolidation of personal data as they trust that the information will not be misused—but it’s not about trust. Handing one’s personal data over to the “right” entity, whether such entity is public or private, may nevertheless result in such data landing in the “wrong” hands due to hacking or security breaches. Several examples of such breaches have already been documented: in Singapore, for instance, the personal information of over 300,000 customers of karaoke company K Box was made publicly available. Not even the government is immune: in 2014, over 1,500 SingPass accounts (which allow citizens to manage everything, from their taxes to applications for state subsidies for training courses, via a government portal) were compromised.

## 5.3 The Consequences

When such personal data is leaked, the problems that come with it are numerous, and it may not be as innocent as others knowing more than one would like - it may affect one’s ability to find jobs or secure insurance coverage, to name a few - and Singapore’s existing data protection laws don’t do enough to mitigate them. These risks are exacerbated by how the buying and selling of personal data have become commonplace. In January 2018, a former telemarketer, Sharon Tang, became the first person in Singapore to be convicted for the unauthorised sale of personal data. Claims by collectors that data will be “anonymised” are of little help as people can be “re-identified through a few pieces of information about them”; one method of which would be by matching data points against other publicly-available information.

## 5.4 An Example

In one notable case in 2006, Netflix issued an open challenge for people to devise a better movie recommendation algorithm than its existing one. As part of this challenge, the video streaming company released its database of 10 million movie ratings made by 500,000 users. This database was anonymised—Netflix had replaced subscribers’ information with random names and numbers—yet two graduate students were able to identify selected users simply by cross-referencing the ratings in Netflix’s dataset against public film reviews made on the Internet Movie Database (IMDb). Among other things, they were able to find out users’ names, movie rental records and even socio-political views (as derived from comment histories on public threads).

# 6. Can privacy be resolved under the provisions of the Personal Data Protection Act/law of confidential information?

The Personal Data Protection Act (PDPA) establishes data protection laws that explain how personal data of people should be handled. This Act ensures that any organization that collects, uses and distributes personal data complies. The Personal Data Protection Act follows three concepts

Consent, Purpose and Reasonableness.

## 6.1 Consents:

Organisations may collect, use or disclose personal data only with the individual's knowledge and consent

## 6.2 Purpose:

Organisations may collect, use or disclose personal data in an appropriate manner for the circumstances, and only if they have informed the individual of the purposes for the collection, use or disclosure

## 6.3 Reasonableness:

Organisations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.

PDPA will issue punishment to organisations or individuals who failed to comply with the PDPA laws. An example of this would be the Singhealth Data Breach where the personal information of 1.5 million was compromised. The PDPA who fined Singhealth for $250,000 stated that even if their information security was handled by a vendor it was their responsibility to take care of the personal information they collect.

Another incident where personal data law was breached was the Karaoke Chain K-Box. A total of eleven organisations were found not complying with the PDPA laws. One of the companies was fined $50,000 for not having sufficient security measures while five of the organisation was given a stern warning and the remaining six told to enhance their current security system or face more fines up to $50,000.

The organisation is not only to comply with the PDPA but also any relevant personal data law that is related to their industry. A law firm must ensure that they comply with PDPA when they receive personal information from their client and at the same time not to break their client-attorney privilege. The hospital must ensure that the patient's medical record must be kept confidential while following their own company policy regarding personal information.

The development of technology has changed the way personal information is collected and kept. The current laws may not be enough to protect our personal information but with the growth of technology so does the PDPA. It will continue to add, change and modify its laws in order to better protect our personal information. Therefore I think privacy can be resolved with the Personal Data Protection Act.

# 7. Conclusion

The effectiveness of the Computer Misuse Act and other data protection regimes are bogged down by a deeper issue - the desire to commoditise data. Despite all the possible risks, the government wants to continue to make it easier for our data to be traded, especially between its own associated organisations, due to the government’s quest to make Singapore a “Smart Nation”.

Nationwide digitisation offers many benefits, some of which are significant and indisputable; while at the same time, it poses real risks to Singaporeans’ privacy and security and therefore, paradoxically, inconveniences citizens by forcing them to be ever-conscious about what they might be, advertently or inadvertently, revealing about themselves.

Thus, while it is useful for people to exercise a degree of personal responsibility by adopting measures to better protect personal privacy and data security, such measures are merely stop-gap solutions -- they do nothing to address the larger issue of how Singapore is headed in policy directions that compromise these things and allow for the government to exert even greater control over Singaporeans’ lives under the guise of being “future-forward” or “smart”. What is instead needed is a sea change in mentality or, as one commentator puts it, “[w]e have to create a culture of respect for personal data at all levels of society”.

*End of Report*

**References:**

Definitions, C. and Hope, C. (2020). *What is Computer Crime?*. [online] Computerhope.com. Available at: https://www.computerhope.com/jargon/c/compcrim.htm [Accessed 22 Jan. 2020].

Solove, D. (2020). *10 Reasons Why Privacy Matters - TeachPrivacy*. [online] TeachPrivacy. Available at: https://teachprivacy.com/10-reasons-privacy-matters/ [Accessed 27 Jan. 2020].

Elena Chong (2015) Ex-sports betting trader who tweaked football odds jailed [online] Available at https://www.straitstimes.com/singapore/courts-crime/ex-sports-betting-trader-who-tweaked-football-odds-jailed [Access 28 Jan 2020]

Amir Hussain (2016) Ex-bank officer jailed for misuse of database [online] Available at https://www.straitstimes.com/singapore/courts-crime/ex-bank-officer-jailed-for-misuse-of-database [Access 28 Jan 2020]

Tay, J. (2018). *Singapore’s Flawed Data Privacy Regime - New Naratif*. [online] New Naratif. Available at: https://newnaratif.com/research/singapores-flawed-data-privacy-regime/ [Accessed 28 Jan. 2020].

TODAY, “Hackers leak data of over 300,000 K Box members”, 17 September 2014, https://www.todayonline.com/singapore/hackers-leak-data-over-300000-k-box-members

The Straits Times, “More than 1,500 SingPass accounts could have been accessed illegitimately: IDA”, 4 June 2014, http://www.straitstimes.com/singapore/more-than-1500-singpass-accounts-could-have-been-accessed-illegitimately-ida

Irene Tham (2019) Singapore's privacy watchdog fines IHiS $750,000 and SingHealth $250,000 for data breach [online] Available at https://www.straitstimes.com/singapore/singapores-privacy-watchdog-fines-ihis-750000-singhealth-250000-for-data-breach

Personal Data Protection Commission (2012) How does the Personal Data Protection Act work? Accessed 28 Jan 2020 [online] Available at https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview

Ng Jing Ying (2016) Karaoke chain fined S$50,000 for breaching data protection law Accessed 28 Jan 2020 [online] Available at

https://www.todayonline.com/singapore/11-organisations-fined-warned-data-privacy-breaches

The Straits Times, “‘Data monger’ fined $6k by privacy watchdog for selling personal data without notification or consent”, 28 January 2018, http://www.straitstimes.com/singapore/singapore-privacy-watchdog-takes-first-data-monger-to-task

Kevin Sheperdson et al, 88 Privacy Breaches to Beware of: Practical Data Protection Tips from Real-Life Experiences(Marshall Cavendish, 2016) at p. 166

Netflix, “Netflix Prize”, https://www.netflixprize.com/rules.html

Wired, “Why ‘Anonymous’ Data Sometimes Isn’t”, 12 December 2007, https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/

SecurityFocus, “Researchers reverse Netflix anonymization”, 4 December 2007, https://www.securityfocus.com/news/11497. The paper detailing the two students’ methodology and application can be found at <https://arxiv.org/pdf/cs/0610105.pdf>.

larson, j., Clay, R., Lawrence, G., Lawrence, G., Klein, D., parisi, R., Lawrence, G., Leo), M. and Clemens, L. (2020). *How Long Should a Password Be? - Ask Leo!*. [online] Ask Leo!. Available at: https://askleo.com/how\_long\_should\_a\_password\_be [Accessed 28 Jan. 2020].

Bandakkanavar, R. (2020). *Causes of CyberCrime and Preventive Measures - Krazytech*. [online] Krazytech. Available at: https://krazytech.com/technical-papers/cyber-crime [Accessed 28 Jan. 2020].

Sso.agc.gov.sg. (2020). *Computer Misuse Act - Singapore Statutes Online*. [online] Available at: https://sso.agc.gov.sg/Act/CMA1993 [Accessed 30 Jan. 2020].

Rohaidi, J. (2020). *Exclusive: Tan Kiat How's vision for data | GovInsider*. [online] GovInsider. Available at: https://govinsider.asia/security/tan-kiat-how-imda-ceo-regulatory-sandboxes/ [Accessed 3 Feb. 2020].

[Hariz Baharudin](https://www.straitstimes.com/authors/hariz-baharudin) (2019) *Singapore Red Cross website hacked, over 4,200 affected* [online] Available at https://www.straitstimes.com/singapore/spore-red-cross-website-hacked-over-4200-affected

[Accessed 3 Feb 2020]

CNA. (2020). *Commentary: Our convenience is coming at a (security) cost*. [online] Available at: https://www.channelnewsasia.com/news/commentary/commentary-our-convenience-is-coming-at-a-security-cost-9435976 [Accessed 3 Feb. 2020].