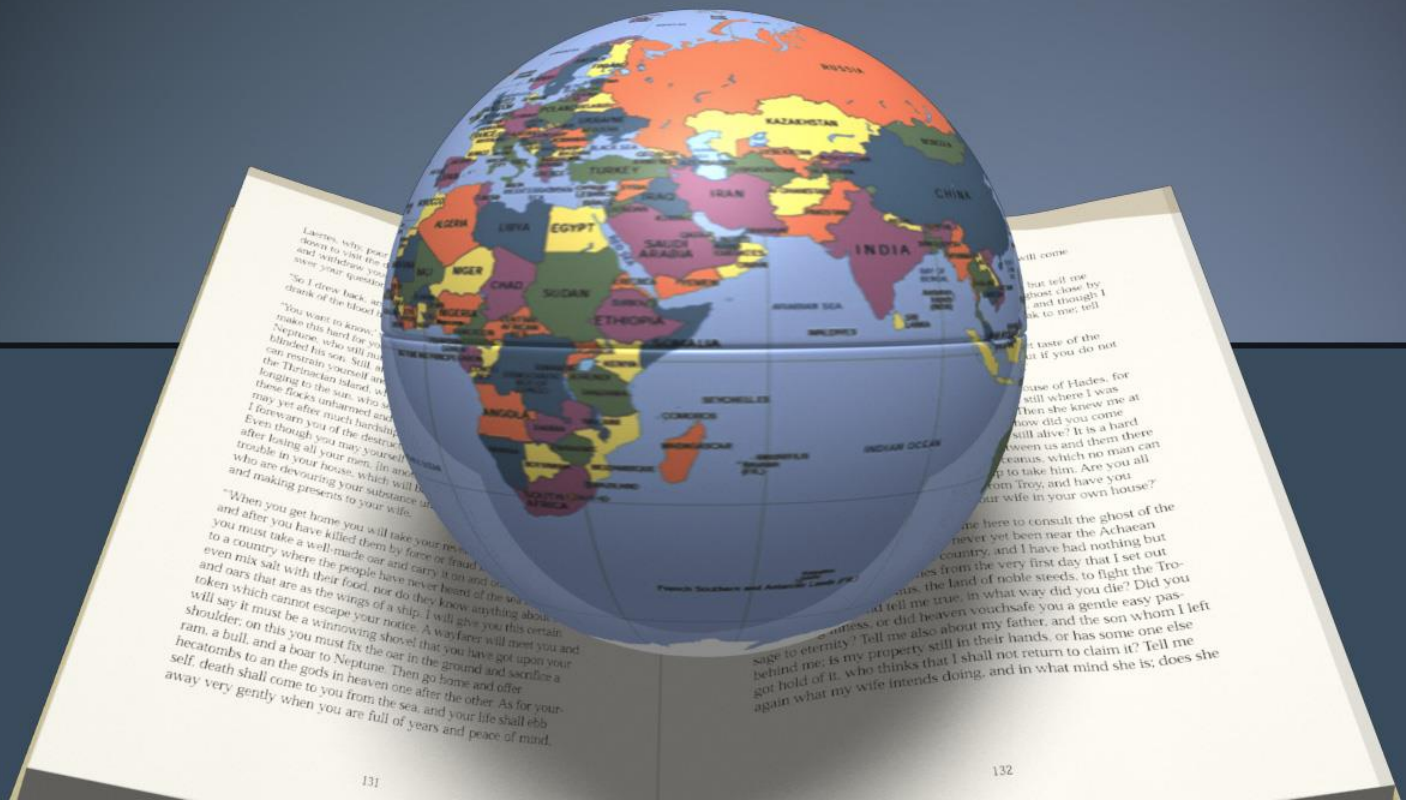
IT1218/IT1769

Law & Ethics of IT

- Lecture 07 : Singapore Technology Laws



7.1
ELECTRONIC TRANSACTION ACT (ETA)

7. Singapore Technology Laws

Overview

- An introduction to laws relating to information technology
- An understanding of legal issues relating to technology

Outline

7.1 Electronic Transaction Act (ETA)

7.2 Computer Misuse and Cybersecurity Act (CMCA)

7.3 Personal Data Protection Framework (PDPF)

7.1 What is Electronic Transaction Act (ETA)

ETA is an act of buying or selling something or sending money electronically, especially over the internet

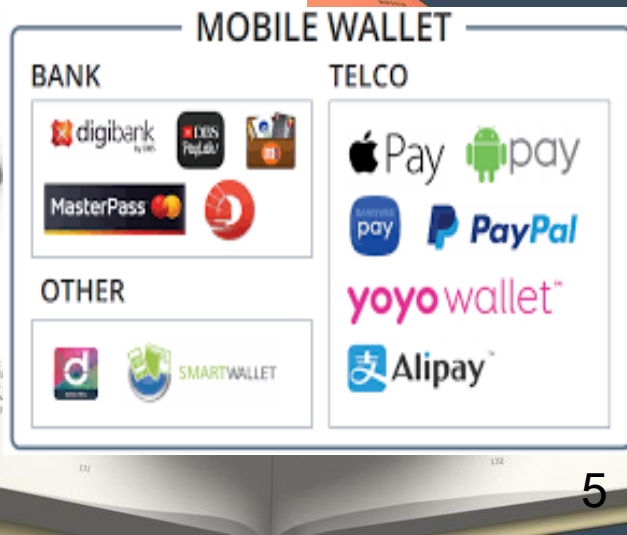
Source:
https://dictionary.cambridge.org/zhs/%E8%AF%8D%E5%85%B8/%E8%8B%B1%E8%AF%AD/electronic-transaction

Many businesses and consumers are unclear about how consumer protection laws can be enforced when electronica transaction take place across borders.

7.1 Electronic Transaction Act (ETA)

Why there is a need for ETA ?

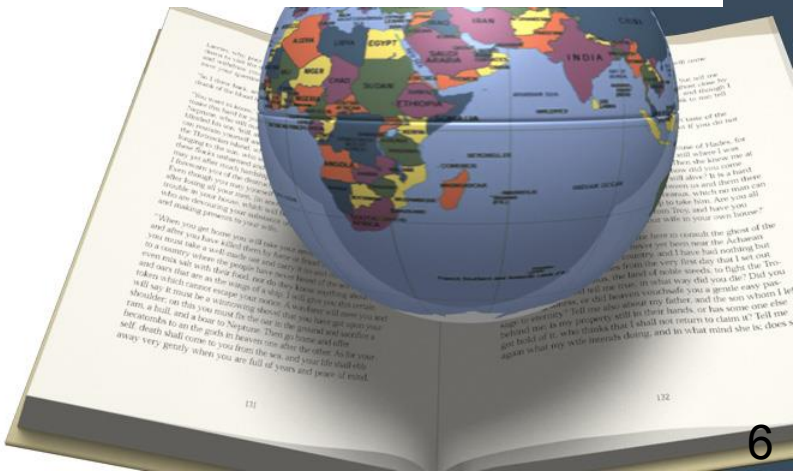
- Enact a commercial code for electronic commerce transactions;
- Provide for a public key infrastructure;
- Enable electronic applications and licences for public sector; and
- Clarify network service providers' (NSP) liability



7.1 ETA (Overview)

Coverage

- Electronic records and signatures
- Liability of Network Service Provider (NSP)
- Electronic contracts
- Secure electronic records and signatures
- Effects of digital signatures
- General duties relating to digital signatures

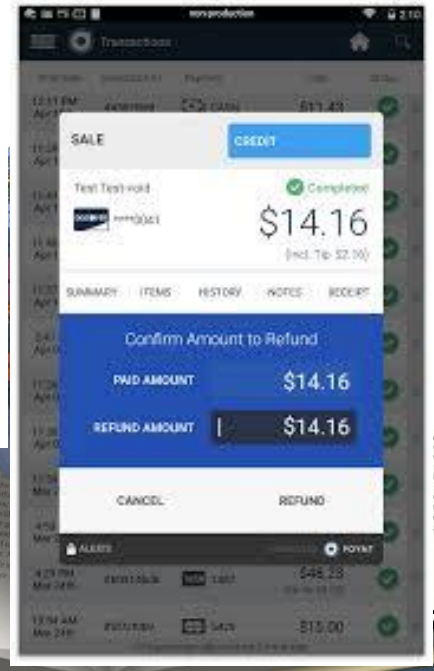


7.1 ETA – Electronic Signature & Record

Definition of an electronic signature & electronic record

"electronic signature" means any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record;

"electronic record" means a record generated, communicated, received or stored by electronic, magnetic, optical or other means in an information system or for transmission from one information system to another;



7.1 ETA – Electronic Contracts

Electronic Contracts

- Parties may legally contract using electronic records
- Such records will not be denied any validity or enforceability by reason of it being an electronic record
- Only certain classes of transactions may not use electronic records, for example drafting & executing a will, contracts for sale or other disposition of immovable property (buying and selling properties), negotiable instruments, declarations of trusts or power of attorney and document of title.
- Formation of contracts using automated system without human intervention allowed.

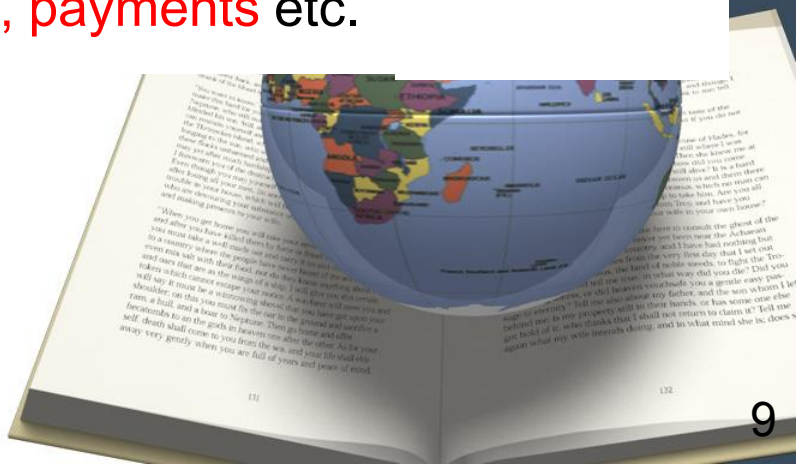
(Note: A **negotiable instrument** is a document guaranteeing the payment of a specific amount of money, either on demand, or at a set time, with the payer usually named on the document. e.g. Bank cheque)

(Note: Documents of **title** include a bill of lading (Acknowledgment the receipt of a shipment of goods), dock warrant, dock receipt, warehouse receipt, and order for the delivery of goods).

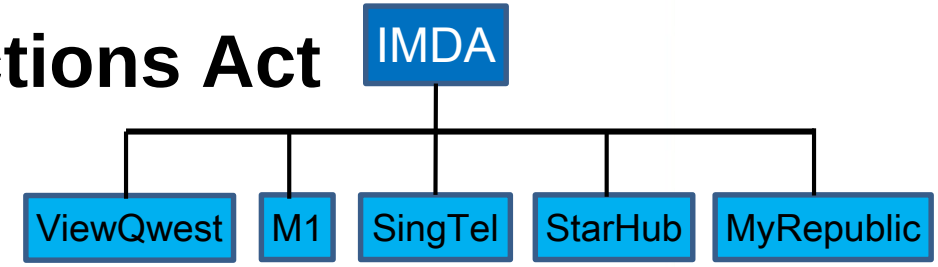
7.1 ETA – Electronic Contracts

Electronic Contracts

- Original documents can be retained as electronic records (for example accounting, tax records – 7 years)
- Record dispatched when it leaves the system or received by the other party – allow movement of emails between servers instead of a closed system
- Advertisement on the Internet – just offers – not capable of “acceptance” unless stated
- E- government : Government may transact electronically such as issuing licenses, payments etc.



7.1 Electronic Transactions Act



Liability of Network Service Providers (NSP)

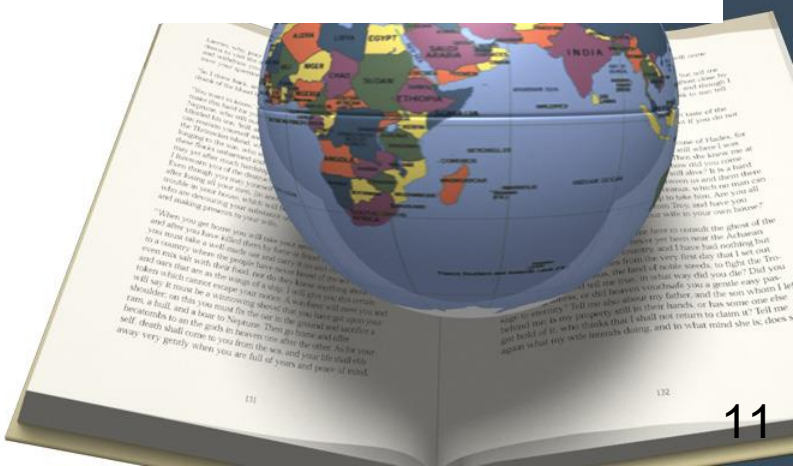
- Network service providers (ISPs such as Singtel etc.) may **NOT** be liable for innocently carrying defamatory materials or materials which infringed the intellectual property rights of others.
- NSP specifically protected under ETA - by freeing the network service provider from liability on a claim of making or disseminating third party materials or infringing rights subsisting on such materials.
- ETA will exempt the network service provider from liability only if it provided mere access for such materials.
- **Not exempted if** NSPs play a part in the publication of such materials or the infringement of IPR rights.

7.1 Secure Electronic Transaction (SET)c

Secure Electronic Record and Signature

- ETA allows commercially reasonable security procedure agreed to by the parties as forming the basis for a secure electronic record and signature.

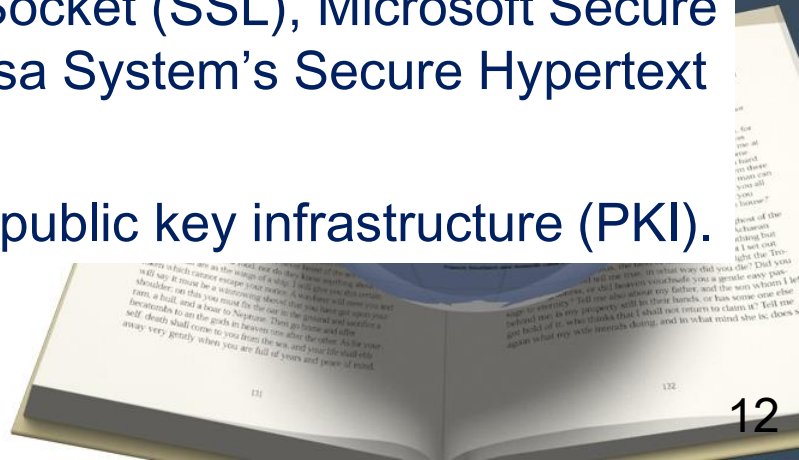
- In digital signatures, it is recognized as the signature of the person to whom it relates. The Act presumes that the signature was affixed with the intention of signing and approving the electronic record.



7.1 Secure Electronic Transaction (SET)

How Secure Electronic Transaction was processed?

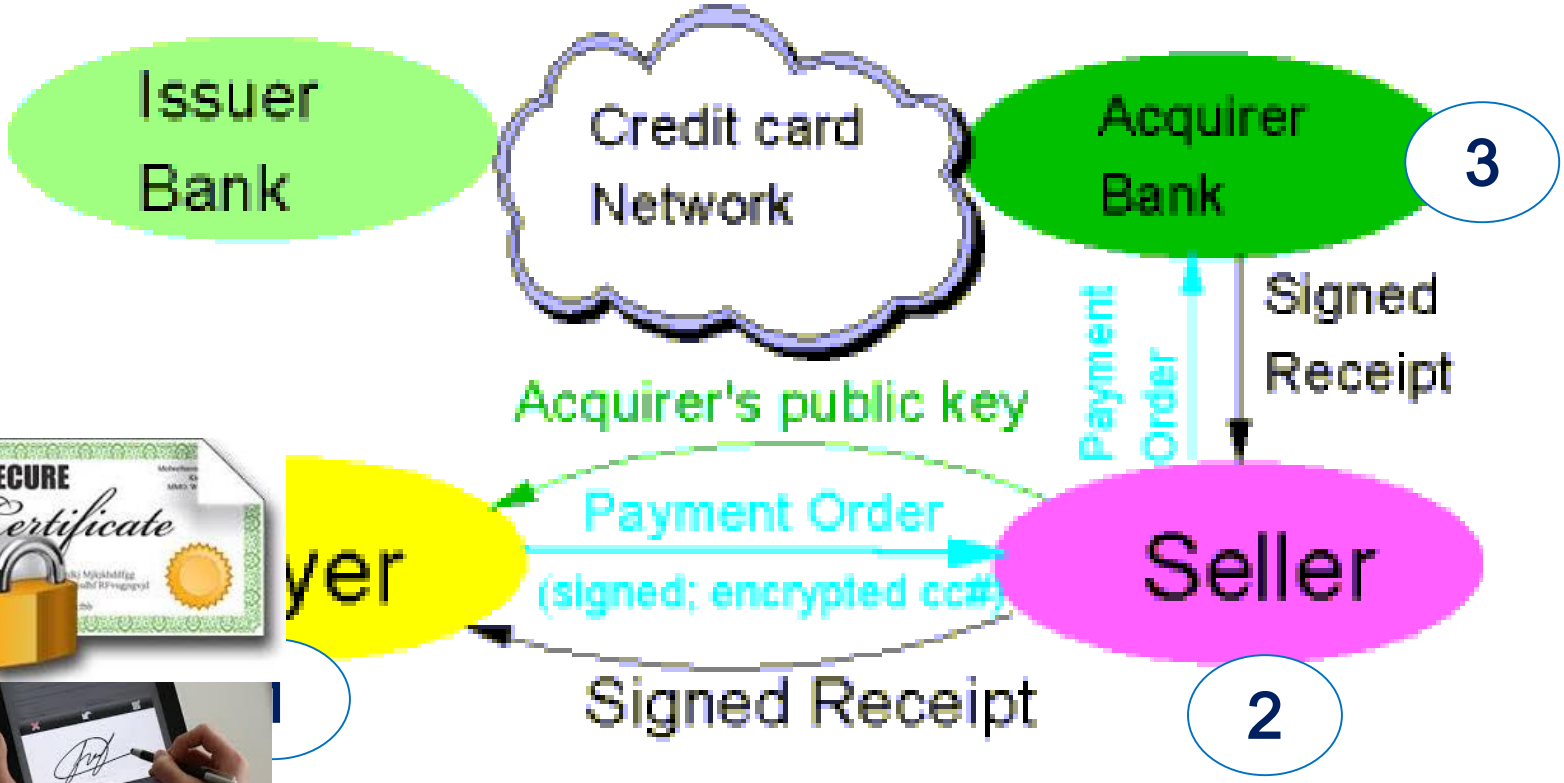
- Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet.
- It was supported initially by Mastercard, Visa, Microsoft, Netscape and others.
- With SET, a user is given an electronic wallet (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensure privacy and confidentiality .
- SET makes use of Netscape's Secure Socket (SSL), Microsoft Secure Transaction Technology (STT) and Terisa System's Secure Hypertext Transfer Protocol (S-HTTP).
- SET uses some but not all aspects of a public key infrastructure (PKI).



7.1 Secure Electronic Transaction (SET)

How Secure Electronic Transaction was processed?

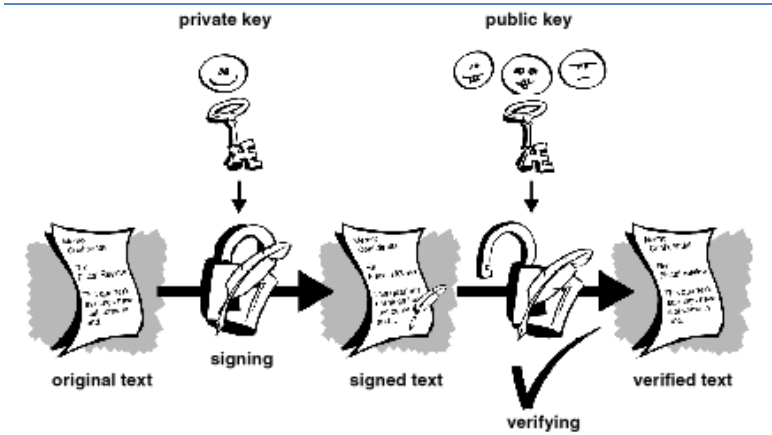
Credit Card Payments with Secured Electronic Transaction (SET)



7.1 SET – Digital Signature

Digital signature in Secured electronic transaction

- Digital signatures mathematically transform an electronic message into a code
- Each message for which a digital signature is affixed may have a different identification code even if all the signatures are signed by the same person using the same key.
- The digital signature allows for a two-key system; a private key and a public key. The recipient of the information will know that it is an authentic record when he applies to the record that has been signed off with the private key held by the originator, the public key of the originator being publicly known.
- Where the two keys match, there is verification and authentication of the record.



Merchant – Hold private key

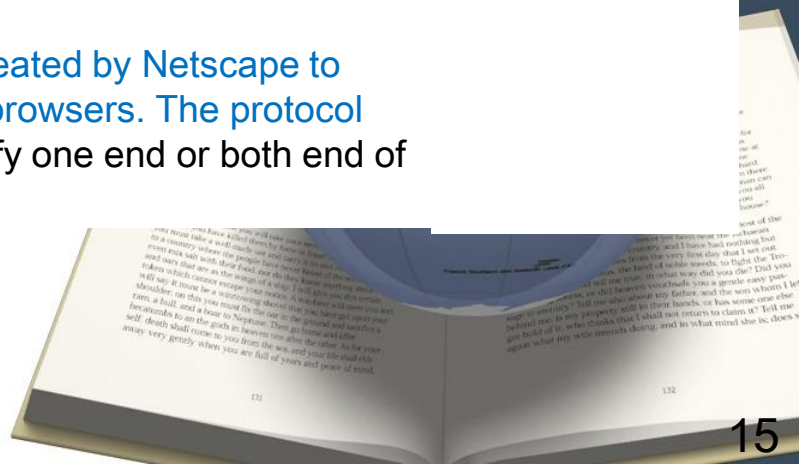
Buyer – Hold public key

7.1 SET – Digital Certificates

The Public Key Infrastructure (PKI)

- The public key is issued and managed by a certification authority. The Act allows for the establishment of certification authorities whose role is to issue public key certificates to those who sign the documents for the purpose of the verification. The certification authority therefore act as a trusted third party who is acceptable to all parties in respect of the secure transactions.
- New technologies like biometrics are included in the Act

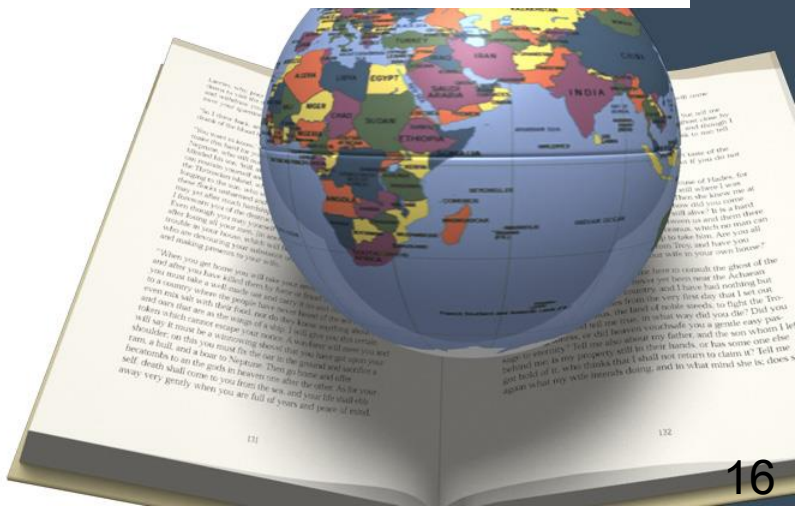
Note: The Secure Socket Layer (SSL) protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party, a Certificate Authority (CA), to identify one end or both end of the transactions



7.1 Electronic Transactions Act

Conclusion

- The ETA is part of the overall attempt by the government to strengthen the infrastructure framework for electronic transactions in Singapore to make Singapore an e-commerce hub
- The way forward increasingly is for our society to have *paperless transactions*.

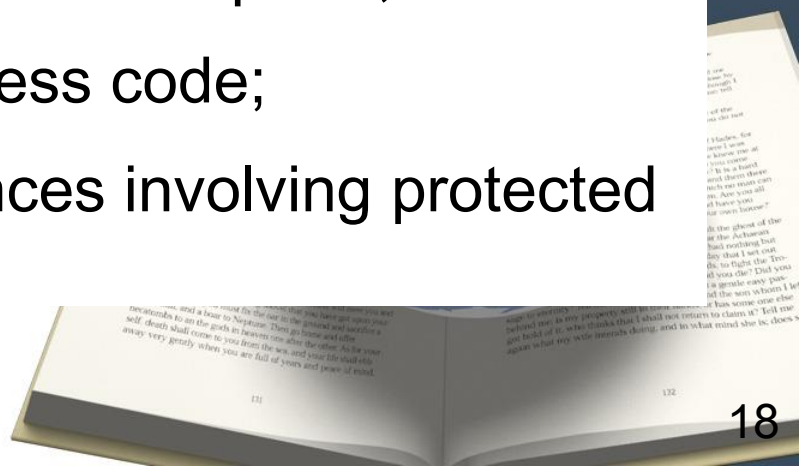


7.2
COMPUTER MISUSE
&
CYBER SECURITY ACT
(CMCA)

7.2 Computer Misuse and Cybersecurity Act (CMCA)

Coverage

- Unauthorized access to computer material;
- Access with intent to commit or facilitate commission of offence;
- Unauthorised modification of computer material;
- Unauthorised use or interception of computer service;
- Unauthorised obstruction of use of computer;
- Unauthorised disclosure of access code;
- Enhanced punishment for offences involving protected computers;



Cybersecurity Coverage

Coverage:

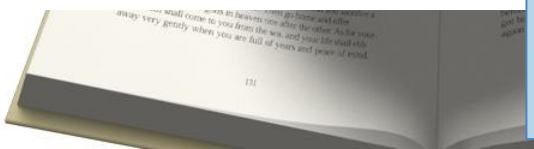
a) **Dealing in hacked information is an offence.**

For persons to obtain or deal in personal information obtained illegally from a computer (e.g. hacking) for illegitimate purposes;

b) **Dealing in hacking tools with criminal intent is an offence.**

For persons to obtain hacking tools to commit or facilitate the commission of a computer offence, as well as deal in hacking tools, intending it to be used for committing or facilitating the commission of a computer offence; and

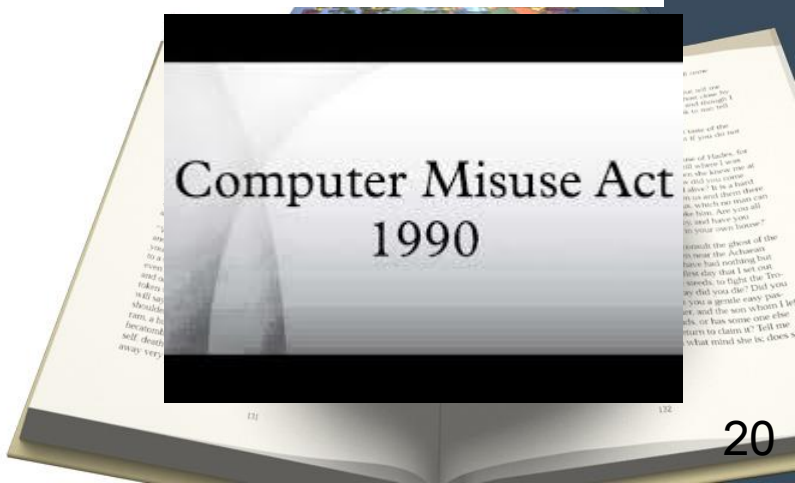
c) For persons to commit criminal acts while overseas, against a computer located overseas, if the act causes or creates a significant risk of serious harm in Singapore.



7.2 Computer Misuse and Cybersecurity Act (CMCA)

Coverage

- Territorial scope;
- Counter action to prevent or countering threats to Singapore;
- Provision to protect informers in legal proceedings; and
- Arrest by police without warrant.



7.2 Computer Misuse and Cybersecurity Act (CMCA)

Unauthorised access to computer material

- It is an offence if a person knowingly changes, erases, copies, moves, prints or even uses a *program or data* in a computer without permission. The sentence on conviction is a *fine not exceeding $5,000* or to *imprisonment for a term not exceeding 2 years* or both.
- Example - entering the company's system to copy or delete client's data after his permission to do so has been revoked.

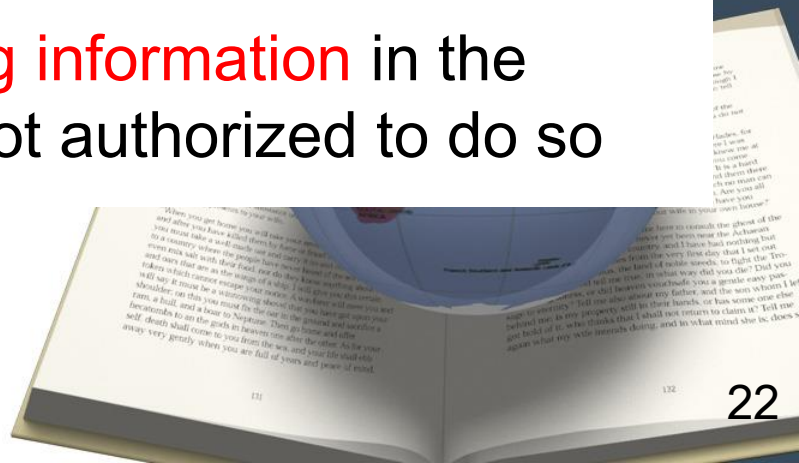
7.2 Computer Misuse and Cybersecurity Act (CMCA)

Unauthorised modification of computer material

- This is an offence whereby a person knowingly and without authority does an act which causes the contents of a computer to be changed, erased, added to or impairs the normal operations of the computer.

  The sentence on conviction is a *fine not exceeding $10,000* or *to imprisonment for a term not exceeding 3 years* or to both.

- Example – vandalizing, changing information in the server, folders etc. when he is not authorized to do so



7.2 Computer Misuse and Cybersecurity Act (CMCA)

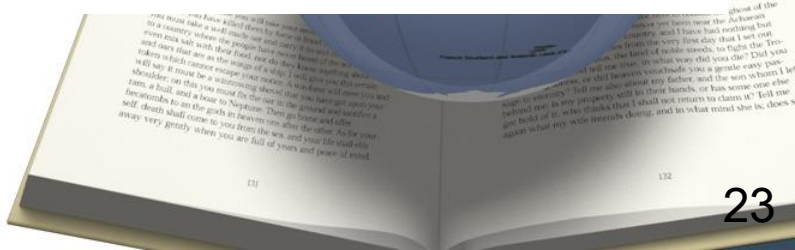
Unauthorised use or interception of a computer service

- Any person who knowingly and without authority:

  (i) secures access to any computer to obtain services; or
  (ii) intercepts, records or listens to a function or a communication to or from a computer; or
  (iii) uses any other device to carry out acts (i) or (ii), shall be guilty of an offence and

  the sentence on conviction is a *fine not exceeding $10,000* or to *imprisonment for a term not exceeding 3 years* or both.

- Example - using ***"free" broadband service of your neighbor*** who did not secure his wireless broadband.



7.2 Computer Misuse and Cybersecurity Act (CMCA)

Unauthorised obstruction of the use of a Computer

Any person who, knowingly and without authority or lawful excuse:

(i) interferes, interrupts or obstructs the use of a computer; or

(ii) impedes or prevent access to, or impairs the usefulness or effectiveness of a program or data stored in a computer

Shall be guilty of an offence punishable upon conviction to a *fine not exceeding $10,000* or *imprisonment for a term not exceeding 3 years* or both.

Example – denial of service by "***email flooding***".

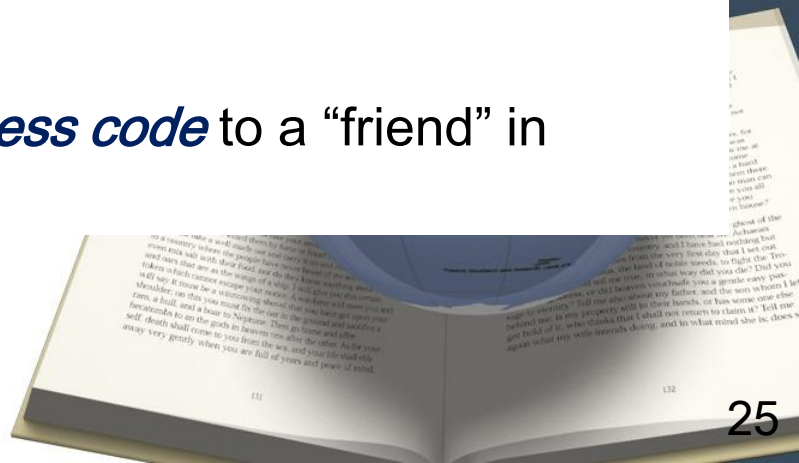
7.2 Computer Misuse and Cybersecurity Act (CMCA)

Unauthorised disclosure of access code

- It is an offence to disclose one's access code to any program or data held in any computer if the disclosure was for a wrongful gain, unlawful purpose or with the knowledge that it is likely to cause wrongful loss to any person.

  If found guilty, a *fine not exceeding $10,000* is imposed or *imprisonment for a term not exceeding 3 years* or both.

- Example – giving your ***company's access code*** to a "friend" in exchange for money



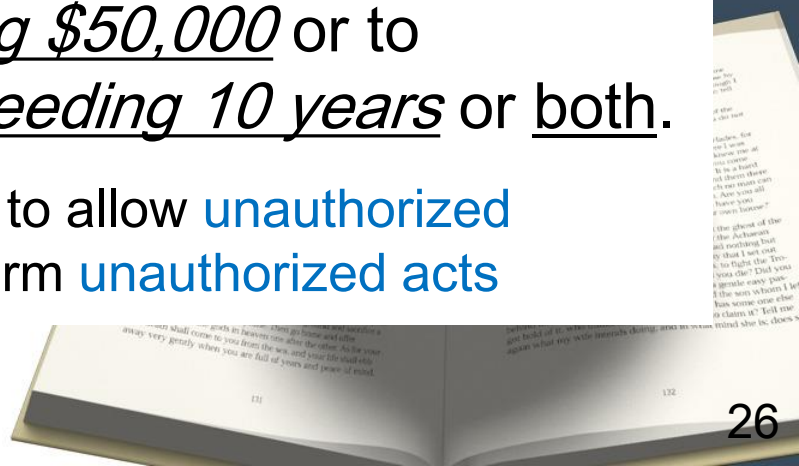
7.2 Computer Misuse and Cybersecurity Act (CMCA)

Access with intent to commit or facilitate commission of an offence

- Any person who changes, erases, copies, moves, prints or even uses a *program* or *data* from a computer, whether or not he was authorised to do so,

  with the intention to commit an offence involving property, fraud, dishonesty or which causes bodily harm shall be guilty of an offence and the sentence on conviction is a *fine not exceeding $50,000* or to *imprisonment for a term not exceeding 10 years* or both.

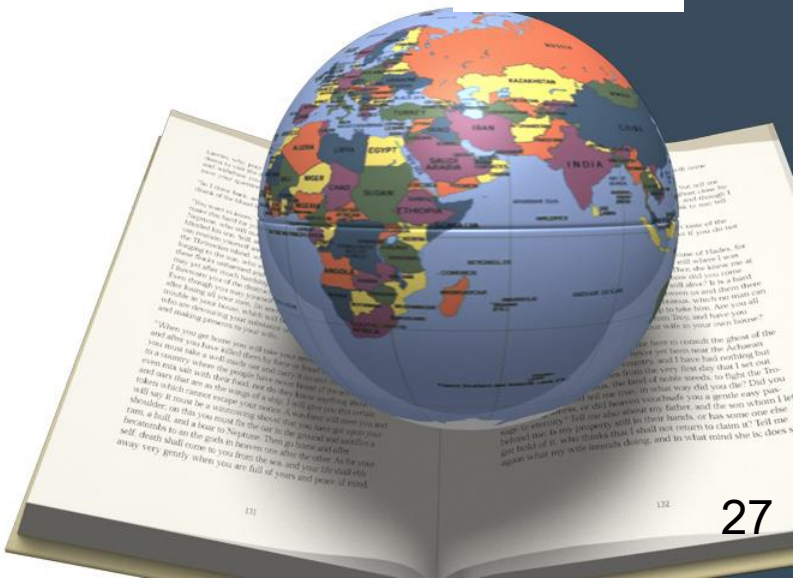
- Example – using your ***company's pass*** to allow unauthorized person/s into your server room to perform unauthorized acts



7.2 Computer Misuse and Cybersecurity Act (CMCA)

Territorial scope

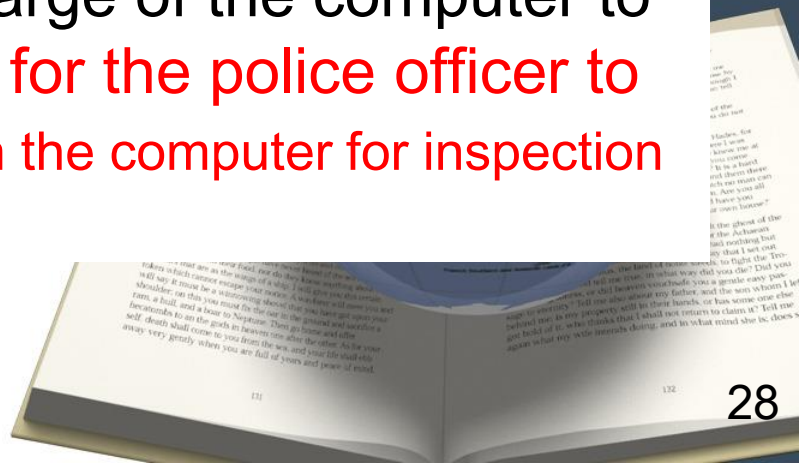
- The Act applies to persons/ acts committed within Singapore and any offence committed under the Act outside of Singapore may be treated as *being committed within Singapore* *if the target (program, server, data etc) is located in Singapore*.



7.2 Computer Misuse and Cybersecurity Act (CMCA)

Police Investigative Powers (Criminal Procedure Code)

- If a police officer has reasonable cause to suspect that a computer is or has been used in connection with any offences under the Act he may be:
  - ✓ Be entitled at any time to have access to and inspect the operation of the computer; and
  - ✓ With the consent of the Public Prosecutor may require the person having charge of the computer to release information sufficient for the police officer to decrypt scrambled data held in the computer for inspection and investigation.



7.3
PERSONAL DATA PROTECTION ACT (PDPA)

7.3 Personal Data Protection Act (PDPA)

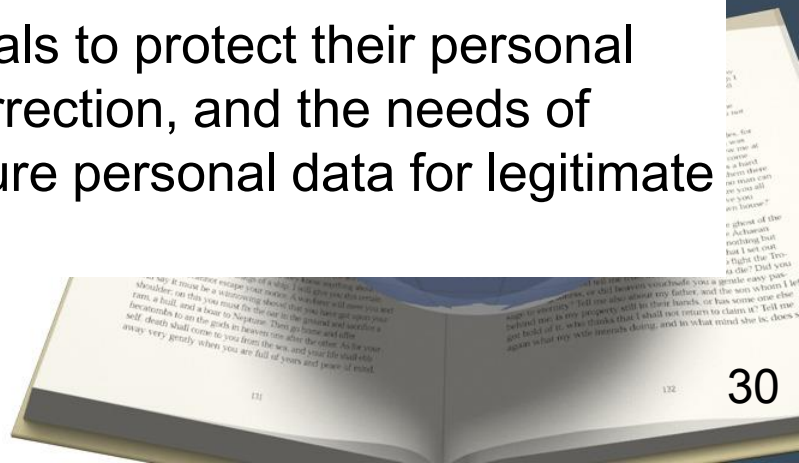
Definition of Personal Data?

Personal data" refers to data about an individual who can be identified from that data; or from that data & other info to which the organisation has or is likely to have access.

(e.g. NRIC, Phone, Address, Incomes etc.)

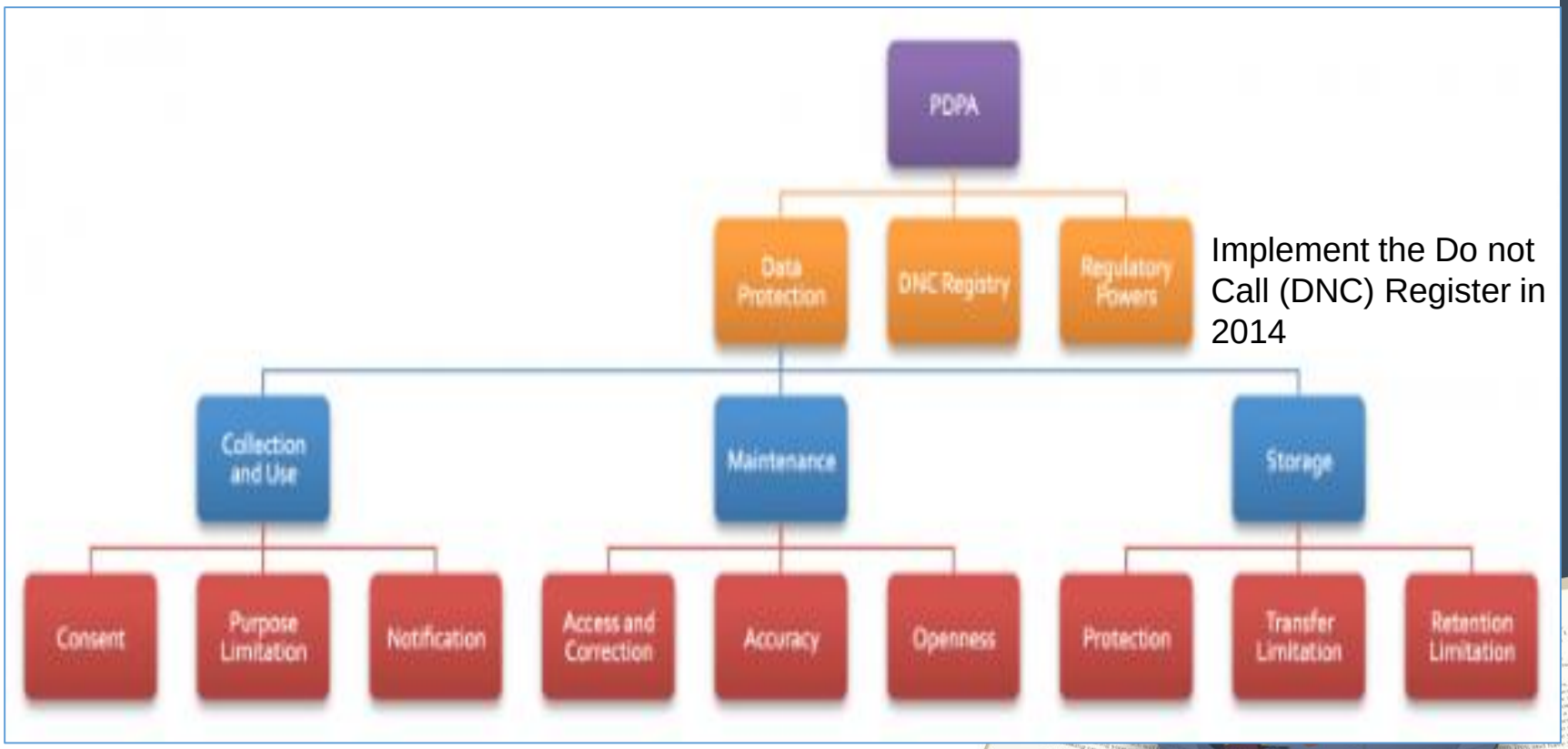
What is PDPA?

- The Personal Data Protection Act (PDPA) aims to regulate the collection, use and disclosure of personal data of individuals and between organizations.
- It recognizes both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organizations to collect, use or disclosure personal data for legitimate and reasonable purposes.



7.3 Personal Data Protection Act (PDPA)

The governing area of PDPA?



Implement the Do not Call (DNC) Register in 2014

Source: http://learn.asialawnetwork.com/2016/11/14/definite-guide-singapore-pdpa-personal-data-protection-act/

7.3 Personal Data Protection Act (PDPA)

Reasons for Personal Data Protection:

a) Consumer Interest

- More intelligent & pervasive technologies;
- Individual have less control over their data & growing concerns;
- Burden on consumers to pursue suspected misuse after the fact.

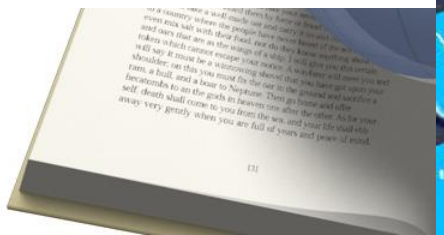
b) Economic Interest

- Strengthen Singapore's overall competitiveness;
- Enhance attractiveness as trusted hub for growing industries, e.g. data management & data processing;
- Facilitate cross-border transfer.

7.3 Personal Data Protection Act (PDPA)

Data Protection Rules:

- Organizations may only collect, use or disclose data *if consent is given for purposes specified*
- *Consent must be validly given*
- *Withdrawal of consent is allowed*
- *Individual shall have access to & be able to request correction of own data*
- *Data to be reasonably accurate and protected.*
- *Do not retain data when not needed for legal or business purposes*



7.3 Personal Data Protection Act (PDPA)

Duration of Personal Data:

- According to The EU General Data Protection Regulation (GDPR), Organisations will need to be more considered and disciplined in their retention of individuals personal data.
- Personal data shall be kept for no longer than is necessary for the purposes for which it is being processed.
- For those personal data stored should be limited to a strict minimum and that time limits should be established by the data controller for deletion of the records

Source: https://www.dpnetwork.org.uk/gdpr-data-retention-guide/

Personal Data of Deceased Individuals:

- Only disclosure & safekeeping rules apply;
- Protection for up to 10 years after death.

7.3 Personal Data Protection Act (PDPA)

Penalties of breaching PDPA:

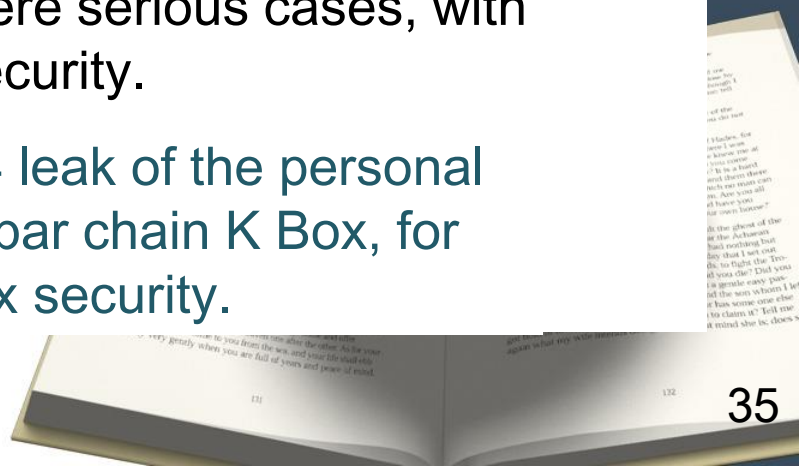
- An organization or person that commits an offence under section 51(3)(b) or (c) of the PDPA is liable to:

  - For individual : fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both; and

  - For an organization, : to a fine not exceeding $100,000.

- According to the news report in July 2017, the Personal Data Protection Commission has taken enforcement action against 300 organizations to date with most of them receiving an advisory notice. But over 30 of them were serious cases, with organizations fined or rapped for lax security.

- A notable case us the September 2014 leak of the personal data of 317,000 customers of karaoke bar chain K Box, for which the firm was fined $50,000 for lax security.



7.3 Personal Data Protection Act (PDPA)

Singapore

27 Jan 2017

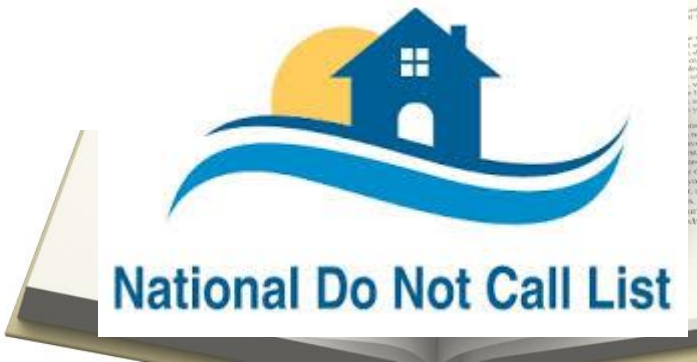
2 companies fined S$10,000 each for breaching data protection rules

JP Pepperdine Group and Propnex Realty were both imposed the financial penalty after failing to secure customers' personal information on their IT systems, thus making them available publicly.

7.3 Personal Data Protection Act (PDPA)

DNC - How it works ….

1. Individual registers phone number with DNC (Do-Not-Call) registry;
2. Phone number is added to DNC register;
3. Organization must send their list of numbers to DNC.
4. DNC registry checks through the lists
5. Consumers will not be contacted unless they withdraw their registration or terminate their service



7.3 Personal Data Protection Act (PDPA)

When does the Personal Data Protection Act Come into Effect?

- The PDPA takes effect in phases starting with the provisions relating to the formation of the PDPC on 2 January 2013.
- Provisions relating to the DNC Registry came into effect on 2 January 2014 and the main data protection rules on 2 July 2014.

- End of Lecture 07

- Electronic Transactions Act (ETA)
  - Electronic records, electronic signatures & electronic contracts
  - Liability of Network Service Provider (NSP)
- Computer Misuse and Cybersecurity Act (CMCA)
  - Unauthorized access/ modification/ use/ obstruction of use/ disclosure of computer materials.
- Personal Data Protection Act (PDPA)
  - Reason for personal data protection
  - Data protection rule
  - Penalty of beaching PDPA
  - Do Not Call Register (DNC)