CSA

4. Appointment of Commissioner of Cybersecurity and other officers
5. Duties and functions of Commissioner
6. Appointment of authorised officers

Part 3 CRITICAL INFORMATION INFRASTRUCTURE

7. Designation of CII
8. Power to obtain infomartion to ascertain if computer, etc., fulfils criteria of CII
9. Withdrawal of designation of CII
10. Furnishing of infomation relating to CII
11. Codes of practice amnd standards of performance
12. Power of Commissioner to issue written directions
13. Change in ownership of CII
14. Duty to report cybersecurity incident in respect of CII
15. Cybersecurity audits and risk assessments of CII
16. Cybersecurity exercises
17. Appeal to Minister
18. Appeal to Advisory Panel

Part 4 RESPONSES TO CYBERSECURITY THREATS & INCIDENTS

19. Powers to investigate and prevent cybersecurity incidents, etc
20. Powers to investrigate and prevent serious cybersecurity incidents, etc.
21. Production of identification card by incident response officer
22. Appointment of cybersecurity technical experts
23. Emergency cyberseucirty measures and requirements

Part 5 CYBERSECURITY SERVICE PROVIDERS

24. No person to provide licensable cybersecurity service without licence
25. Licensing officer and assistant licensing officer
26. Grant and renewal of licence
27. Conditions of licence
28. Form and validity of licence
29. Duty to keep records
30. Revocation or suspension of licence
31. Unlicensed cybersecurity service provider not to recover fees, etc
32. Financial penalty
33. Licensing officer to give opportunity to make representations before ordering financial penalty
34. Recovery of financial penalties
35. Appeal to Minister

Part 6 GENERAL

36. Offences by corporations
37. Offences by unincorporated associations or partnerships
38. Powers of investigation
39. Power to enter premises under warrant
40. Jurisdiction of court
41. Composition of offences
44. Protection from personal liability

PDPA

3. Purpose
4. Application of Act

PART II PDPC AND ADMINSTRATION

5. Personal Data Protection Commission
6. Functions of Commission
7. Advisory Committee
8. Delegation
9. Conduct of proceedings
10. Co-operation agreements

PART III GENERAL RULES WITH RESPECT TO PROTECTION OF PERSONAL DATA

11. Compliance with Act
    (3) Designate one or more individuals to be responsible to comply with this
    (5) Make available to public business contact
12. Policies and practices
    (a) Developer and implement policies and practises necessary
    (c) Communicate to its staff info about own's policies
    (d) Make infomation available on request about policies

PART IV COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

13. Consent required
14. Provision of consent
15. Deemed consent
16. Withdrawal of consent
17. Collection, use and disclosure without consent
18. Limitation of purpose and extend
19. Personal data collected before appointed day
20. Notification of purpose

PART V ACCESS TO AND CORRECTION OF PERSONAL DATA

21. Access to personal data
22. Correction of personal data

PART VI CARE OF PERSONAL DATA

23. Accuracy of personal data
24. Protection of personal data
25. Retention of personal data
26. Transfer of personal data outside Singapore

PART VII ENFORCEMENT OF PARTS III TO VI

27. Alternative dispute resolution
28. Power to review
29. Power to give directions
30. Enforcement of directions of Commission in District Court
31. Reconsiderations of directions or decisions
32. Right of private action

Interpretation of PDPA

includes the activity of any organisation, whether or not carried on for purposes of gain, or conducted on a regular, repetitive or continuous basis, bu does not include an individual acting in his personal capacity

"business contact information" means an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes

"data intermediary" means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation

"employment" includes working under an unpaid volunteer work relationship

"individual" means a natural person, whether living or deceased;

"organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not -
(a) formed or recognised under the law of Singapore; or
(b) resident, or having an office or a place of business, in Singapore

"personal data" means data, whether true or not, about an individual who can be identified -
(a) from that data; or
(b) from that data and other info to which the organisation has or is likely to have access;

"private trust" means a trust for the benefit of one or more designated individuals who are friends, or members of the family, of the settlor;

"processing", in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following: (a) recording; (b) holding; (c) organisation, adaptation or alteration; (d) retrival; (e) combination; (f) transmission; (g) erasure or destruction

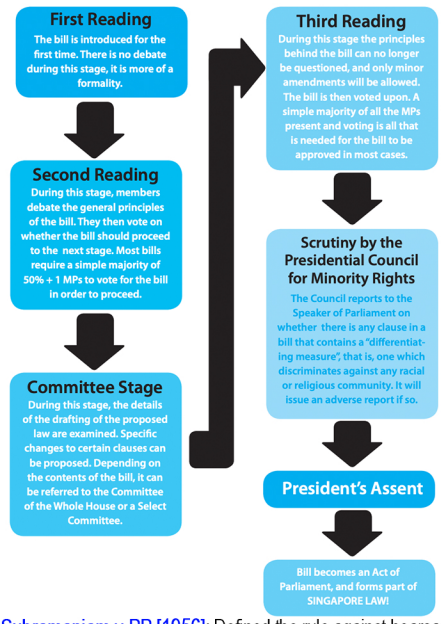
"public agency" includes - (a) the Government, including any ministry, dept, agency, or organ of State; (b) any tribunal appointed under any written law; or (c) any statutory body specified under subsection (2)

"publicly available", in relation to personal data about an individual, means personal data that is generally available to the public, and includes personal data which can be observed by reasonably expected means at a location or an event - (a) at which the individual appears; and (b) that is open to the public;

"evaluative purpose" means - (a) for the purpose of determining the suitability, eligibility or qualifications of the individuals to whom the data relates - (i) for employment or for appointment to office; (ii) for promotion in employment or office or for continuance in employment or office; (iii) for removal from eployment or office; (iv) for admission to an education institution; (v) for the awarding of contracts, awards, bursaries, scholarships, honours or other similar benefits; (vi) for selection for an athletic or artistic purpose; or (vii) for grant of financial or social assistance; (b) for the purpose of determining whether any contract, award, bursary, scholarship, honour or other similar benefit should be continued, modified or cancelled; (c) for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property; or (d) for such other similar purposes as may be prescribed by the Minister

Contradictory

	General Cybersecurity Threat: s 19	Severe Cybersecurity Threat: s 20	Critical Cybersecurity Threat: s 23
Object	•assess (potential) impact of threat/incident •prevent any/further harm •prevent further incident	•risk of significant harm being caused, or risk of disruption to, CII or provision of "essential service" •threat to national security, defence, foreign relations, economy, public health, public safety, public order •threat satisfies 'severity' threshold	serious and imminent threat to essential service, national security, defence, foreign relations, economy, public health, public safety, public order
Computer / System Targeted	any computer/system	CII; "an essential service"; threat to national security etc.; threat/incident of severe nature because of no of persons, computers, value of info, whether or not computers/systems are CII	essential service, national security, defence, foreign relations, economy, public health, public safety, public order
Information	interview any person, produce any information, copy any record, examine any acquainted person	(as previous)	•require any person to provide any information – including design, configuration, operation, cybersecurity, decryption information •provided with any information including real time •report of breach/attempt
Action		•direct any person to carry out remedial measures, or cease action •owner to take any action to assist in investigation •enter premises after giving reasonable notice •assess, inspect computer/system and check/search any data •get assistance from any person •scan for vulnerabilities •take/extract any affected record/program •take possession of any computer/equipment for further examination (even without consent)	•take such measures as may be necessary •power to access computer
Exemption	no breach if done with reasonable care and in good faith (no breach for information subject to right, privilege, immunity, other privilege, contract, rules of conduct)	no breach if done with reasonable care and not wilful misstatement	no breach if without reasonable excuse or if subject to legal privilege (reasonable excuse does *not* include right, immunity, other privilege, contract, rules of conduct)
Immunity	no breach of any contractual obligation for act done/omitted to be done with reasonable care and in good faith and for answering any question		•no liability for act in compliance with s 23 •no breach of legal, contractual or professional restriction
Offence	wilfully misstates or without reasonable excuse refuses to give any information or comply with Magistrate's order: $5,000 or 6 months jail or both	wilfully misstates or without reasonable excuse refuses to give any information or comply with Magistrate's order, or comply with direction or lawful demand: $25,000 or 2 years jail or both	without reasonable excuse fails to take any measure or comply with any requirement, or obstructs a specified person or fails to comply with any direction: $50,000 or 10 years jail or both



• Subramaniam v PP [1956]: Defined the rule against hearsay, page 6 evidence act
- Admit computer record, dismiss hearsay: Roy S Selvarajah v PP [1998] (About abetment of overstaying).The Singapore High Court in the case of Roy S Selvarajah v PP that the computer database records with the Data Processing Centre of the Immigration Department are admissible as "documents" under section 380, CPC. The evidence showed that the principal offence of overstaying was committed as a result of Selvarajah's abetment. Given the need to protect the public interest in deterring would-be offenders from abetting illegal overstayers to remain in Singapore, the sentence imposed was not excessive

2. - (1)
"business entity" means - (a) a corporation as defined in section 4(1) of the Companies Act (Cap.50); (b) an unincorporated association; (c) a partnership; or (d) a limited liability partnership registered under the Limited Liability Partnership Act
"computer system" means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes - (a) an information technology system; and (b) an operation technology system such as an industrial control system, a programmable logic controller, a supervisory controla nd data acquisition system, or a distributed control system
"critical information infrastructure" means a computer or a computer system in respect of which a designation under sect 7(1) is in effect
"cybersecurity" means the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state - (a) the computer or computer system continues to be available and operational; (b) the intergrity of the computer or computer system is maintained; and (c) the integrity and confidentiality of info stored in, processed by or transmitted through the computer is maintained
"cybersecurity incident" means an act or activity carried out without lawful authority on or through a computer or computer system that jeopardieses or adversly affects its cybersecurity or cybersecurity of another computer or computer system;
"cybersecurity program" means any computer program designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of a computer or computer system;
"cybersecurity service" means a service provided by a person for reward that is intended primarily for or aimed at ensuring or safeguarding the cybersecurity of a computer or computer system belonging to another person (A), and includes the following: (a) to (k)
"cybersecurity threat" means an act or activity (whether known or suspected) carried out on or through a computer or computer system that may imminently jeopardise or affect adversely, without lawful authority, the cybersecurity of that or another computer or computer system
"cybersecurity vulnerabillity" any vulnerability in a computer or computer system that can be exploited by one or more cybersecurity threats;
"essential service" means any service essential to the national security, defence, or foreign relations, economy, public health, public safety or public order of Singapore, and specified in the First Schedule;
"owner", in relation to CII, means the legal owner of the CII and, where the CII is jointly owned by more than one person, includes every joint owner
2 - (2) A person does not provide a cybersecurity service only because the person - (a) sells, or sells licences for, cybersecurity programs intentded to be installed by a user without the assistance of the seller for the protection of the cybersecurity of a user's computer; or (b) provides services for the management of a computer network or computer system, that are aimed at ensuring the availability of or enhancing the performance of the computer network or computer system.

• PP v Ang Soon Huat [1990]: Drug trafficiking.The computer printouts of the results of the scientific tests were real evidence and not hearsay evidence The computers in the scientific instruments not only recorded but also processed and calculated the information fed into them and oral evidence had been given in regard to those matters.
Gimpex Ltd v Unity Holdings Business Ltd [2015]: The Sucofindo Report was nonetheless admissible under s 32(1)(b)(iv) of the Evidence Act as a document that was compiled by a person acting in the ordinary course of a trade, business, profession or occupation based on information supplied by other persons. Section 32(1)(b)(iv) did not require the person who prepared the document to have personal knowledge of the information contained therein. In exercising its discretion to exclude admissible hearsay evidence pursuant to s32(3) of the Evidence Act, the issue at hand was whether admissible evidence should be excluded because other countervailing factors outweighed the benefit of having the evidence admitted. There were serious issues concerning the reliability of the Sucofindo Report. The defendant failed to produce evidence that sufficiently assured the court that there was a minimal degree of reliability in the Sucofindo Report. It was thus in the interest of justice not to admit the Sucofindo Report

Interpretation of CSA

By: Gan Chin Yao I 2019 May

Secured access

Access – statutory definition

- CMA s 2 Interpretation.
- (2) For the purposes of this Act, a person secures access 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 shall be read accordingly.

Unauthorised access

- CMA s 2 Interpretation.
- *(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 -*
- *(a) he is not himself entitled to control access of the kind in question to the program or data; and*
- *(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.*

Modification

- *(7) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer —*
  - *(a) any program or data held in the computer concerned is altered or erased;*
  - *(b) any program or data is added to its contents; or*
  - *(c) any act occurs which impairs the normal operation of any computer,*
- *and any act which contributes towards causing such a modification shall be regarded as causing it.* Writer of virus also counted
- (8) Any modification referred to in subsection (7) is unauthorised if --
  - *(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and*
  - *(b) he does not have consent to the modification from any person who is so entitled.*

Interpretation

.—(1) In this Act, unless the context otherwise requires —

"computer" means an electronic, magnetic, optical, electrochemical, or other 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 device or group of such interconnected or related devices, but does not include —

(*a*) an automated typewriter or typesetter;

(*b*) a portable hand-held calculator;

(*c*) a similar device which is non-programmable or which does not contain any data storage facility; or

(*d*) such other device as the Minister may, by notification in the *Gazette*, prescribe;

"computer output" or "output" means a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement or representation of fact —

(*a*) produced by a computer; or

(*b*) accurately translated from a statement or representation so produced;

"computer service" includes computer time, data processing and the storage or retrieval of data;

"damage" means, except for the purposes of section 13, any impairment to a computer or the integrity or availability of data, a program or system, or information, that —

(*a*) causes loss aggregating at least $10,000 in value, or such other amount as the Minister may, by notification in the *Gazette*, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account;

(*b*) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons;

(*c*) causes or threatens physical injury or death to any person; or

(*d*) threatens public health or public safety;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"electro-magnetic, acoustic, mechanical or other device" means any device, apparatus or program that is used or is capable of being used to intercept any function of a computer;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;

"intercept", in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;

"program or computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

[21/98]

cite format: s 6(1)(a) of the Computer Misuse Act (Cap 50A)

s 3: Unauthorised access
- **s 3(1): Unauthorised access, knowingly**
- **s 3(2): Damaged caused as a result**

s 4: Aggravated access (access with intent to commit offence)
- **s 4(1): Access with intent to commit offence**
- **s 4(4): For s 4, immaterial Authorisied/Unauthorised**

s 5: Unauthorised modification
- **s 5(1) Knows will cause unauthorised modification**
- **s 5(2) Damaged caused (e.g. trojan)**
- **s 5(4) Immaterial modification is temp or perm**

s 6: Unauthorised use or interception (e.g. phone cloning, use other ppl internet)
- **s 6(1)(a) Unauthorised access, knowingly, to obtain computer service**
- **s 6(1)(b) Unauthorised interception of any function of a computer, knowingly (keylogger, port scanner)**
- **s 6(1)(c) knowingly, use a computer or device to commit (a) or (b)**
- **s 6(2) Damage caused**

s 7: Unauthorised obstruction (e.g. DDoS, encryption)
- **s 7(1)(a) knowingly, unauthorised, interfere or interrupt computer use**
- **s 7(1)(b) knowingly, unauthorised, impedes or prevent access to data**
- **s 7(2) Damage caused**

s 8: Unauthorised disclosure of access code
- **s 8(1) Knowingly, unauthorised, disclosed for wrongful gain/ unlawful purpose**

s 8A: Supplying personal info obtained in contravention of certain provisions

Must be used for committing a crime then counted
- **s 8A(1)(a) Knowingly, or believed to, obtained personal info of another person**
- **s 8A(1)(b) Supplies personal info**

s 8B: Obtaining items for use in certain offences
- **s 8B(1)(a) Obtain item with intent to use it to commit s3,4,5,6,7**
- **s 8B(1)(b) Supply the item for it to be used to commit s3,4,5,6,7**

s 9: Enhanced punishment for protected computers

s 10: Abetments (incite/assist others to commit crime) and attempts are offences

	Original	Enhanced (damage caused)
S 3 – unauthorised access	Fine: $5,000, Jail: 2 years, or both 2nd and subsequent conviction: Fine: $20,000, Jail: 5 years, or both	Fine: $50,000, Jail: 7 years, or both
S 4 – access with intent to commit offence	Fine: $50,000, Jail: 10 years, or both	Fine: $50,000, Jail: 7 years, or both
S 5 – unauthorised modification	Fine: $10,000, Jail: 3 years, or both 2nd and subsequent conviction: Fine: $20,000, Jail: 5 years, or both	Fine: $50,000, Jail: 7 years, or both
S 6 – unauthorised use/interception	Fine: $10,000, Jail: 3 years, or both 2nd and subsequent conviction: Fine: $20,000, Jail: 5 years, or both	Fine: $50,000, Jail: 7 years, or both
S 7 – unauthorised obstruction	Fine: $10,000, Jail: 3 years, or both 2nd and subsequent conviction: Fine: $20,000, Jail: 5 years, or both	Fine: $50,000, Jail: 7 years, or both
S 8 – unauthorised disclosure	Fine: $10,000, Jail: 3 years, or both 2nd and subsequent conviction: Fine: $20,000, Jail: 5 years, or both	

- Piggybacking wifi: March 2007, Garyl Tan, 18 month's probation, piggyback neighbor wifi in order to engage in online chatting
- Trojan, keylogger: Nguyen Van Phi Hung, jailed 1 year 8 months
- Keylogger: SMU JD student Kotsaga used keylogger copy lecturer's userID and pw, deleted his and 18 studens' exam scripts, jailed 2 months
- Help another person to illegally access a computer system to obtain confidential information: Eric Tan and former classmate working for Starhub, each fined 20k
- Memorise gf internet banking pin while helping her, logged in and xfer money to himself, jailed 21 months, 4 charges under CMA. Yang Yingze, 20, 2005
- Unauthorised access: PP v Muhammad Nuzaihanbin Kamal Luddin, pleaded guilty to 3 charges: s 3(1), s 6(1)(a), s 5(1), 30 months' probation appeal by PP, eventually become an aggregate sentence of 4 months, 2 months for each charges. 17 yrs old
  s 3(1): Secured system administrator privileges (root access) on Swiftech Automation Pte Ltd's server, Cloud4
  s 5(1): Secured system administrator privileges on Singapore Cable Vision Ltd's server, Brahms, and modified the contents of the file 'inetd.conf'
  s 6(1)(a): Operated an Internet Relay Chat service on Cloud4 server by utilizing port 31337
- Unauthorised access: Lim Siong Khee v PP [2001], Lim accessed his girlfriend email account and sent emails to her friends detailing their intimate relationship. GF gave Lim her account only for help in Europe, but not subsequent access back in Singapore
  s 3(1): convicted for 5 months jail, subsequent appeal increased this to 12 months
- s 7 unauthorised obstruction: Tan Hian Chye placed 1908 false bids on eBay to disrupt activies of more than 1000 sellers in Feb and March 2002. Fined $27k, 9k each on 3 charges under CMA
- s 7 unauthorised obstruction: Spam mail. PP v Kendrick Tan [2000]. Kendrick Tan sent 2500 emails in 2 and half hours to 3 separate and different HDB mailboxes. Fined $30k, $4 per email
- s 4 access with intent to commit an offence. PP v Law Aik Meng [2007]. Law was charged with engaging with accomplices to cause a computer to secure access to the data in the Central Computer System of Development Bank of Singapore Limited (DBS) with the intention of using that access to commit theft of cash
- s 3(1) charge. Tan Chye Guan Charles V PP [2009]. Tan inserted a thumbdrive and copied file from DSTA project manager without his consent. File was commercially sensitive, and not military sensitive, hence not charge under s 9.

R v Bow Street Magistrates: 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
Authority to access one piece of data could not be treated as authority to access other data of the same kind, and that since the employee has been given authority to access only that part of the company's data, the access by her of other data was unauthorised

Lim Siong Khee v PP [2001]: Consent to access a programme or data had to come from the person who was entitled to access the data in question, and in free web-based email, the account holder. Access without authority depends on the account holder, not the computer system owner or provider.

PP v Muhammad Nuzaihanbin Kamal Luddin [1999]: the High Court judge took the view that probation, designed to afford young offenders rehabilitation by removing their opportunity to re-offend, was not an appropriate response to computer offending.

Nature of Offence	Legislation	Section
Theft of funds, economic losses	Penal Code	s 378 (theft) s 383 (extortion) s 403 (criminal misappropriation of property) s 405 (criminal breach of trust)
Personal harm or injury	Penal Code	s 319 (hurt) s 376E (sexual grooming) s 503 (criminal intimidation) s 590 (outraging modesty)
Privacy and data protection	Personal Data Protection Act	s 51 (offences)
Disturbing social order	Penal Code	s 298 (words wounding religious/racial feelings) s 298A (promoting enmity on grounds of religion/race or prejudicial to maintenance of harmony)
	Sedition Act	s 4 (offences)
Copyright infringement	Copyright Act	s 136 (offences for commercial dealings) s 260 (RMI offences) s 261C (TPM offences)

Hacking	Unauthorised access to programs and data – s 3, CMA; access with intent to commit offence – s 4, CMA
Trojan, worms, virus attacks	Unauthorised modification – s 5, CMA
Collecting user-IDs, passwords via trapdoors, spyware, spoofing, intercepting communications	Unauthorised interception – s 6, CMA
Denial of service ('DOS') attacks , distributed DOS	Unauthorised obstruction of use of computer – s 7, CMA
Sale or trade in passwords or means of gaining access	Unauthorised disclosure of access codes – s 8, CMA
Attacks against infrastructure computers	Protected computers – s 9, CMA
Cyberattack attempts	Abetments and attempts – s 10, CMA

Whereas: taken into consideration
Case: legal dispute between parties brought before court for adjudication
Actus reus: External act or physical element
Mens rea: internal act, mental element of a person's intention to commit a crime, or knowledge that one's action or lack of action would cause a crime to be commited.
Expressio unius est exclusion alterius: Expression of one thing is exclusion of another
Ejusdem generis: "of the same kind" –if list of specific items is followed by general class, the general class only applies to same kind of specific items listed.
E.g. No automobiles, trucks, tractors, motorcyles and other motor-powered-vehicle motor-powered vehicle would not include airplanes, since list of specific items is of land-based transport
Lex nil frustra facit: "the law does nothing in vain". interpretation given that avoids an absurd or pointless result
Noscitura sociis: "it is known by its companions" – the meaning of a word is affected by its surrounding words and is interpreted accordingly. E.g. burning, tearing, mutilating or defacing a will is illegal. Can it be partially burnt? Yes, since can be partially torn
Stare Decisis: the principle that cases should be decided according to consistent principled rules so that similar facts will yield similar results, lies at the heart of all common law systems. Follow legal ruling in previous court case.
Horizontal stare decisis: Court adhering to its own precedent
Vertical stare decisis: Court applies precedent from a higher court
Ratio decidendi: the reason or the rationale for the decision. Binding, unlike Obiter Dictum.
Obiter Dictum: A judge's expression of opinion, not essential to decision therefore not legally binding as a precedent
Utres magis valeat quam pereat: "that the thing may rather have effect than be destroyed". better to give written provision some effect harmoniously with other written laws than to give ineffect
Separation of power split into: Legislature(make law, President, Parliament), Judicial(interpret law, Supreme Court, Subordinate Court), Executive(excecute law, President, Cabinet, Minister)
How to prove facts: The adversarial process, the evidential process (prove by evidence), the evaluation process (burden of proof, standard of proof)
Inquisitorial system: court is actively involved in investigating facts of case, i.e. court can question defense, prosecutors, witnesses.
Adversarial system: judges focus on the issues of law and procedure, act as referee between the 2 parties fighting each other, rarely ask witnesses qn directly.
Syntactic ambiguity: linguistic syntax can be ambiguous, e.g. or means and
Semantic ambiguity: words can have more than one meaning, e.g. whats a road?
Aids to statutory interpretation: Expressio unius est exclusion alterius, Ejusdem generis, Noscitura sociis, Utres magis valeat quam pereat, Lex nil frustra facit
Lessig'sFour Modalities: Law, code, markets, norms
Preparation (vulnerability scanning, dumpster diving), Input validation (buffer overflow, sql injection, canonicalization, XSS), Software tampering (virus, worm, Trojan horse, backdoor, zeroday exploit), Authentication (spoofing, man in middle, keylogger, skimming), Authorisation (privilege escalation, rootkit), communications management (piggybacking, spyware)
Affidavit: a written statement confirmed by oath or affirmation, for use as evidence in court.
Best Evidence Rule: holds an original copy of a document as superior evidence. The rule specifies that secondary evidence, such as a copy or facsimile, will be not admissible if an original document exists and can be obtained
Circumstancial evidence: however, is evidence that does not point directly to a fact and requires an inference in order to prove that fact.
Direct evidence: any evidence that directly proves or disproves a fact. The most well-known type of direct evidence is a testimony from an eye witness
Discovery: pre-trial procedure in a lawsuit in which each party can obtain evidence from the other party or parties by means of discovery devices such as interrogatories, requests for production of documents, requests fo
Electronic discovery: Refers to discovery in litigation or govt investigations which deals with the exchange of information in electronic format (ESI).
Evidence: Oral, documentary, real
Hearsay: an out of court statement offered to prove the truth of the matter asserted. Exclusionary rule.
Legally relevant: Every fact that is legally relevant is also logically relevant but every logically relevant fact may not be necessarily legally relevant.". Means can admit as evidence
Probative: a term used in law to signify "tending to prove."
Rules of evidence: Rules that tell us how facts are proven in a legal proceedings. encompasses the rules and legal principles that govern the proof of facts in a legal proceeding. concerned with the quantum (amount), qu
Privacy: The ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively.
Subpoena: a writ ordering a person to attend a court.

By: Gan Chin Yao I 2019 May