
LEGAL ASPECTS OF INFORMATION SECURITY

IFS4101

WEEK 10, WELLY TANTONO, DIS, SOC, NUS

SUMMARY OF COMPETENCIES LEARNED

- Singapore's system of governance and its rules of governance (i.e., Singapore laws)
- How to read and interpret case law and statutes
- How to analyze facts to identify potential breaches of the law
- Computer Misuse Act
- Introduction to Intellectual Property Laws
- Information security's impact on forensic investigations (Evidence Act)
- Today: E-Commerce Laws and Introduction to Data Protection

LAWS AFFECTING E-COMMERCE

LAWS THAT AFFECT E-COMMERCE

- Electronic Transactions Act 2010
- Spam Control Act 2007
- Laws regulating advertisements
- Remote Gambling Act 2014
- Protection from Harassment Act 2014
- Protection from Online Falsehoods and Manipulation Act 2019
- Defamation Act

ELECTRONIC TRANSACTIONS ACT 2010

PURPOSES

Purposes and construction

3. This Act is to be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes:

- a) to **facilitate** electronic **communications** by means of **reliable electronic records**;
- b) to **facilitate** electronic **commerce**, to **eliminate barriers** to electronic commerce **resulting from uncertainties** over **writing and signature requirements**, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;
- c) to facilitate **electronic filing** of documents with public agencies, and to promote **efficient delivery by public agencies of services** by means of reliable electronic records;
- d) to **minimise** the incidence of **forged** electronic records, intentional and unintentional alteration of records, and **fraud** in electronic commerce and other electronic transactions;
- e) to help to **establish uniformity of rules**, regulations and standards regarding the authentication and integrity of electronic records;

PURPOSES

... Purposes and construction

- a) to promote **public confidence in the integrity and reliability** of electronic records and electronic commerce, and to foster the **development of electronic commerce through the use of electronic signatures** to lend **authenticity and integrity** to correspondence in any electronic medium;
- b) to **implement** the United Nations Convention on the Use of Electronic Communications in International Contracts adopted by the General Assembly of the United Nations on 23 November 2005 and to make the law of Singapore on electronic transactions, whether or not involving parties whose places of business are in different States, consistent with the provisions of that Convention;
- c) to **adopt** the UNCITRAL Model Law on Electronic Transferable Records adopted by the United Nations Commission on International Trade Law on 13 July 2017 in its application to an electronic transferable record, whether the electronic transferable record is issued or used in Singapore or outside Singapore

PARLIAMENTARY DEBATES

- “There are certain classes of documents or transactions that may not be ready for such an immediate change. Hence, insofar as Part II and Part IV of the Bill are concerned, it is provided in clause 4 that in certain matters such as wills and documents of title, the electronic records, signatures and contract provisions do not apply. This **does not, however, prevent the courts from recognising the use of electronic documents in these matters on a case-by-case basis.** Eventually, when public confidence in electronic transactions grows, the Bill may be widened to include such documents.”
- “A digital signature, when affixed to an electronic document, has two essential properties. It **confirms that a document has not been tampered with since the time the signature was fixed. It also identifies the person who fixed the signature. Traditional hand-written signatures do not perform these functions with the same degree of certainty.** It is therefore justifiable to **afford some evidentiary presumptions on digital signatures and the documents on which they are affixed, if these signatures are created in accordance with a secure procedure.**”

DEFINITIONS

“**communication**” includes any statement, declaration, demand, notice, request, offer or the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract;

“**electronic**” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities;

“**electronic communication**” means any communication that the parties make by means of electronic records;

“**electronic record**” means a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another;

“**record**” means information that is inscribed, stored or otherwise fixed on a tangible medium or that is **stored** in an electronic or other medium and is **retrievable in perceivable form**;

“**originator**”, in relation to an electronic communication, means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage (if any) but does not include a party acting as an intermediary with respect to that electronic communication;

EXCLUDED MATTERS

Excluded matters

4.—(1) The provisions of this Act specified in the first column of the First Schedule do not apply to any rule of law requiring writing or signatures in any of the matters specified in the second column of that Schedule.

(2) The Minister may, by order in the Gazette, amend the First Schedule.

Excluded matters mentioned in the First Schedule include:

- The creation or execution of a will
- The creation, performance or enforcement of an indenture, declaration of trust or power of attorney, with the exception of implied, constructive and resulting trusts
- Any contract for the sale or other disposition of immovable property, or any interest in such property
- The conveyance of immovable property or the transfer of any interest in immovable property.

ABILITY TO ABROGATE APPLICATION OF ETA

Party Autonomy

5.—(1) Nothing in Part 2 affects any rule of law or obligation requiring the agreement or consent of the parties as to the form of a communication or record, and (unless otherwise agreed or provided by a rule of law) such **agreement or consent may be inferred from the conduct of the parties**.

(2) Nothing in Part 2 prevents the parties to a contract or transaction from —

- (a) **excluding the use** of electronic records, electronic communications or electronic signatures in the contract or transaction by agreement; or
- (b) **imposing additional requirements** as to the form or authentication of the contract or transaction by agreement.

(3) Subject to any other rights or obligations of the parties to a contract or transaction, the parties may, by agreement —

- (a) exclude section 6, 11, 12, 13, 14, 15 or 16 from applying to the contract or transaction; or
- (b) derogate from or vary the effect of all or any of those provisions in respect of the contract or transaction.

LEGAL RECOGNITION OF ELECTRONIC RECORDS

6. To avoid doubt, it is declared that information is not to be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.


Question: Why do you think there is a need to establish this as a part of the law?

 ensure that the electronic records coming in are given the same level of presumptions as in the evidence act idea

otherwise electronic record would be rejected and useless

AS A SUBSTITUTE FOR “WRITING”

Requirement for writing

7. Where a rule of law requires information to be written, in writing, to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained in the electronic record  **accessible so as to be usable for subsequent reference.**

Question: What does “in writing” mean? See Cambridge Dictionary.

SIGNATURE CAN BE DOCUMENTED ELECTRONICALLY

Requirement for signature

8. Where a rule of law requires a signature, or provides for certain consequences if a document or a record is not signed, that requirement is satisfied in relation to an electronic record if —

- (a) a method is used to **identify the person** and to **indicate that person's intention** in respect of the information contained in the electronic record; and
- (b) the method used is either —
 - (i) as **reliable as appropriate** for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
 - (ii) **proven in fact** to have fulfilled the functions described in paragraph (a), by itself or together with further evidence.

RETENTION OF ELECTRONIC RECORDS

Retention of electronic records

9.—(1) Where a rule of law requires any document, record or information to be retained, or provides for certain consequences if it is not, that requirement is satisfied by retaining the document, record or information in the form of an electronic record if the following conditions are satisfied:

(a) the information contained therein **remains accessible so as to be usable for subsequent reference;**

(b) the electronic record is **retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;**

(c) such information (if any) as enables the **identification of the origin and destination of an electronic record and the date and time when it was sent or received,** is retained; and

(d) any additional requirements relating to the retention of such electronic records specified by the public agency which has supervision over the requirement for the retention of such records are complied with.

(2) An obligation to retain any document, record or information in accordance with subsection (1)(c) does not extend to any information necessarily and automatically generated solely for the purpose of enabling a record to be sent or received.


RETENTION OF ELECTRONIC RECORDS

- (3) A person may satisfy the requirement mentioned in subsection (1) by using the services of any other person, if the conditions in paragraphs (a) to (d) of that subsection are complied with.
- (4) Nothing in this section applies to —
 - (a) any rule of law which expressly provides for the retention of documents, records or information in the form of electronic records; or
 - (b) any rule of law requiring that any document, record or information be retained (or which provides for consequences if not) that the Minister, by order in the Gazette, excludes from the application of this section in respect of such document, record or information.

ELECTRONIC RECORDS AS SUBSTITUTES FOR “ORIGINALS”

Provision of originals

10.—(1) Where a rule of law requires any document, record or information to be provided or retained in its original form, or provides for certain consequences if it is not, that requirement is satisfied by providing or retaining the document, record or information in the form of an electronic record if the following conditions are satisfied:

-  there exists **a reliable assurance as to the integrity of the information contained in the electronic record from the time the document, record or information was first made in its final form**, whether as a written document or as an electronic record;
- (b) where the document, record or information is to be provided to a person, the electronic record that is provided to the person is **capable of being displayed to the person**; and
- (c) any additional requirements relating to the provision or retention of such electronic records specified by the public agency which has supervision over the requirement for the provision or retention of such records are complied with.

ELECTRONIC RECORDS AS SUBSTITUTES FOR “ORIGINALS”

(2) For the purposes of subsection (1)(a) —

(a) the criterion for assessing integrity is whether the **information has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display;** and

(b) the standard of reliability required must be assessed in the light of the **purpose for which the information was generated and in the light of all the relevant circumstances.**

(3) A person may satisfy the requirement mentioned in subsection (1) by using the services of any other person, if the conditions in paragraphs (a), (b) and (c) of that subsection are complied with.

(4) Nothing in this section applies to any rule of law requiring that any document, record or information be provided or retained in its original form (or which provides for consequences if not) that the Minister, by order in the Gazette, excludes from the application of this section in respect of such document, record or information.

FORMATION OF CONTRACTS THROUGH ELECTRONIC MEANS

Formation and validity of contracts

11.—(1) To avoid doubt, it is declared that in the context of the formation of contracts, an offer and the acceptance of an offer may be expressed by means of electronic communications.

(2) Where an electronic communication is used in the formation of a contract, that contract is not to be denied validity or enforceability solely on the ground that an electronic communication was used for that purpose.

Question: What is it about the formation of contracts through electronic means that makes the offer and acceptance process questionable requiring legislation to put to rest the doubt as to validity of the contract?

ELECTRONIC COMMUNICATION CAN SERVE AS EVIDENCE OF INTENT

Effectiveness between parties

12. As between the originator and the addressee of an electronic communication, a declaration of intent or other statement is not to be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic communication.

so these conditions will similarly give the presumption that the electronic records are reliable until proven otherwise

in banking - if there is a requirement to ensure that money is being changed in 3 days from the start

- what is considered the start time (t) so that we know if the transaction is compliant with (t+3)

TIME AND PLACE OF DESPATCH AND RECEIPT

13.—(1) The time of despatch of an electronic communication is —

- (a) the time when it **leaves an information system under the control of the originator** or of the party who sent it on behalf of the originator; or
- (b) if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, **the time when the electronic communication is received.**

(2) The time of receipt of an electronic communication is the time when the electronic communication becomes capable of being retrieved by the addressee at an electronic address designated by the addressee.

(3) The time of receipt of an electronic communication at an electronic address that has not been designated by the addressee is the time when the electronic communication becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address.

one example can be the buying and selling of shares - if after pressing the "accept" button then the system goes down - will this "contract" still need to be upheld

TIME AND PLACE OF DESPATCH AND RECEIPT

(4) For the purposes of subsections (2) and (3), an electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the electronic address of the addressee.

(5) An electronic communication is deemed to be **despatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business.**

(6) Subsections (2), (3) and (4) apply even though the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under subsection (5).

INVITATION TO MAKE OFFER

14. A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including a proposal that makes use of interactive applications for the placement of orders through such information systems, is to be considered as an **invitation to make offers**, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

purpose: to help protect merchants - so that trying to buy something will allow the merchant to check and choose to take up the offer or not

example: in the case of online retailers, if there is a listing online but they have no more physical stock - when a buyer buys the item, it would not immediately be the fault of the retailer for not being able to fulfill this order

- instead they can choose to reject this "offer" by quoting that they have no stock and hence not receive any penalty under the law

USE OF AUTOMATED MESSAGE SYSTEMS FOR CONTRACT FORMATION

15. A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, is not to be denied validity or enforceability solely on the ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

ERROR IN ELECTRONIC COMMUNICATIONS

16.—(1) Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made.

(2) Subsection (1) does not apply unless the person, or the party on whose behalf that person was acting —

(a) notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and

(b) has not used or received any material benefit or value from the goods or services (if any) received from the other party.

(3) Nothing in this section affects the application of any rule of law that may govern the consequences of any error other than as provided for in subsections (1) and (2).

SECURE ELECTRONIC RECORDS

17.—(1) If a **specified security procedure**, or a commercially reasonable security procedure agreed to by the parties involved, has been properly applied to an electronic record to verify that the electronic record has not been altered since a specific point in time, such record is treated as a secure electronic record from such specific point in time to the time of verification.

(2) For the purposes of this section and section 18, whether a security procedure is commercially reasonable must be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including

-
- (a) the nature of the transaction;
- (b) the sophistication of the parties;
- (c) the volume of similar transactions engaged in by either or all parties;
- (d) the availability of alternatives offered to but rejected by any party;
- (e) the cost of alternative procedures; and
- (f) the procedures in general use for similar types of transactions.

SECURE ELECTRONIC SIGNATURE

18.—(1) If, through the application of a **specified security procedure**, or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made —

- (a) unique to the person using it;
- (b) capable of identifying such person;
- (c) created in a manner or using a means under the sole control of the person using it; and
- (d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated,

such signature is treated as a secure electronic signature.

(2) Whether a security procedure is commercially reasonable must be determined in accordance with section 17(2).

PRESUMPTIONS RELATING TO SECURE ELECTRONIC RECORDS AND SIGNATURES

- 19.—(1) In any proceedings involving a secure electronic record, it is **presumed, unless evidence to the contrary is adduced**, that the secure electronic record has not been altered since the specific point in time to which the secure status relates.
- (2) In any proceedings involving a secure electronic signature, it is presumed, unless evidence to the contrary is adduced, that —
- (a) the secure electronic signature is the signature of the person to whom it correlates; and
 - (b) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.
- (3) In the absence of a secure electronic record or a secure electronic signature, **nothing in this Part creates any presumption relating to the authenticity and integrity of the electronic record or electronic signature.**

LIABILITY OF NETWORK SERVICE PROVIDERS

26.—(1) Subject to subsection (3), a network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which the network service provider merely provides access if such liability is founded on —

- (a) the making, publication, dissemination or distribution of such materials or any statement made in such material; or
- (b) the infringement of any rights subsisting in or in relation to such material.

(2) Subject to subsection (3), a network service provider shall not be subject to any liability under the Personal Data Protection Act 2012 in respect of third-party material in the form of electronic records to which the network service provider merely provides access.

protecting ISP for the content being held on their infrastructure

LIABILITY OF NETWORK SERVICE PROVIDERS

(3) Nothing in this section affects —

- (a) any obligation founded on contract;
- (b) the obligation of a network service provider as such under a licensing or other regulatory regime established under any written law;
- (c) any obligation imposed under any written law or by a court to remove, block or deny access to any material; or
- (d) any liability of a network service provider under the Copyright Act 2021 in respect of a rights infringement as defined by section 97 of that Act.

(4) In this section —

“provides access”, in relation to third-party material, means the provision of the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access;

“third-party”, in relation to a network service provider, means a person over whom the provider has no effective control. 30

SPAM CONTROL ACT 2007

OBJECT

An Act to provide for the control of spam, which is **unsolicited commercial communications** sent in bulk by email or by text or multimedia messaging to mobile telephone numbers, and to provide for matters connected therewith.

DEFINITIONS

- “electronic address” means an **email address, an instant messaging account** or a mobile telephone number to which an electronic message can be sent;
- “instant messaging account” means an account of a user of an instant messaging service;
- “instant messaging service” means a messaging service that allows a user to exchange messages with other users who are using the service concurrently;

DEFINITION OF SPAM / COMMERCIAL ELECTRONIC MESSAGE

Meaning of “commercial electronic message”

3.—(1) In this Act, a commercial electronic message is an electronic message, where, having regard to —

- (a) the content of the message;
- (b) the way in which the message is presented; and
- (c) the content that can be located using the links, telephone numbers or contact information (if any) set out in the message,

it is concluded that the primary purpose of the message is —

- (d) to offer to supply goods or services;
- (e) to advertise or promote goods or services;
- (f) to advertise or promote a supplier, or a prospective supplier, of goods or services;
- (g) to offer to supply land or an interest in land;
- (h) to advertise or promote land or an interest in land;

DEFINITION OF SPAM / COMMERCIAL ELECTRONIC MESSAGE

- (i) to advertise or promote a supplier, or a prospective supplier, of land or an interest in land;
 - (j) to offer to provide a business opportunity or an investment opportunity;
 - (k) to advertise or promote a business opportunity or an investment opportunity;
 - (l) to advertise or promote a provider, or a prospective provider, of a business opportunity or an investment opportunity;
 - (m) to assist or enable a person, by deception, to dishonestly obtain property belonging to another person;
 - (n) to assist or enable a person, by deception, to dishonestly obtain a financial advantage from another person; or
 - (o) to assist or enable a person to dishonestly obtain a gain from another person.
- (2) For the purposes of paragraphs (d) to (l) of subsection (1), it does not matter —
- (a) whether the goods, services, land, interest or opportunity exists; or
 - (b) whether it is lawful to acquire the goods, services, land or interest, or take up the opportunity.

DEFINITION OF SPAM / COMMERCIAL ELECTRONIC MESSAGE

- (3) Any of the following persons may be the individual who, or entity which, is the sender of the message:
 - (a) the supplier or prospective supplier mentioned in paragraph (f) or (i) of subsection (1);
 - (b) the provider or prospective provider mentioned in paragraph (l) of subsection (1);
 - (c) the first mentioned person in paragraph (m), (n) or (o) of subsection (1).
- (4) Subject to subsection (5), a person who knowingly allows the person's product or service to be advertised or promoted by a sender is deemed to have authorised the sending by the sender of any electronic message that advertises or promotes that person's product or service.
- (5) For the purposes of subsection (4), a person who **takes reasonable steps to stop the sending of any electronic message that advertises or promotes** that person's product or service is deemed not to have authorised the sending of the message.

Question: What type of messages are not covered by this definition?

MEANING OF “ELECTRONIC MESSAGE”

- 4.—(1) In this Act, subject to subsection (3), an electronic message is a message sent to an electronic address.
- (2) For the purposes of subsection (1), it **does not matter —**
- (a) whether the electronic address exists; or
 - (b) whether the message reaches its intended destination.
- (3) For the purposes of this Act, a message is not an electronic message if it is sent by way of a voice call made using a telephone service.

ELECTRONIC MESSAGES SENT TO INSTANT MESSAGING ACCOUNTS

4A. For the purposes of this Act —


- (a) where an electronic message is sent to an instant messaging account; and
- (b) the name used to identify, or which is associated with, that instant messaging account is an email address or a mobile telephone number,

the electronic message is not a message sent to the email address or mobile telephone number (as the case may be) mentioned in paragraph (b).

MEANING OF “UNSOLICITED”

5.—(1) In this Act, an electronic message is unsolicited if the recipient did not —

- (a) request to receive the message; or
- (b) consent to the receipt of the message.

(2) For the purposes of subsection (1), a recipient is not to be treated as having requested to receive the message  consented to the receipt of the message merely because the electronic address of the recipient was given or published by or on behalf of the recipient.

(3) For the purposes of subsection (1), where a recipient of an electronic message, other than an unsolicited electronic message, submits an unsubscribe request, the recipient is not to be treated as having requested to receive or consented to the receipt of any message sent after the expiry of 10 business days after the day on which the unsubscribe request is submitted.

MEANING OF “SENDING IN BULK”

6.—(1) For the purposes of this Act, electronic messages are deemed to be sent in bulk if a person sends, causes to be sent or authorises the sending of —

- (a) more than 100 electronic messages containing the same or similar subject matter during a 24-hour period;
- (b) more than 1,000 electronic messages containing the same or similar subject matter during a 30-day period;
or
- (c) more than 10,000 electronic messages containing the same or similar subject matter during a one-year period.

(2) The Minister may, by order in the Gazette, vary the number of electronic messages specified in subsection (1)(a), (b) or (c).

therefore small business might not fall under spam control act

APPLICATION OF ACT

- 7.—(1) This Act does not apply unless an electronic message has a Singapore link.
- (2) For the purposes of subsection (1), an electronic message has a Singapore link in the following circumstances:
- (a) the message originates in Singapore;
 - (b) the sender of the message is —
 - (i) an individual who is physically present in Singapore when the message is sent; or
 - (ii) an entity —
 - (A) which is formed or recognised under the law of Singapore; or
 - (B) which has an office or a place of business in Singapore;

APPLICATION OF ACT

- (c) the computer, mobile telephone, server or device that is used to access the message is located in Singapore;
 - (d) the recipient of the message is —
 - (i) an individual who is physically present in Singapore when the message is accessed; or
 - (ii) an entity that carries on business or activities in Singapore when the message is accessed; or
 - (e) if the message cannot be delivered because the relevant electronic address no longer exists (assuming that the electronic address existed), it is reasonably likely that the message would have been accessed using a computer, mobile telephone, server or device located in Singapore.
- (3) Despite subsection (1), this Act does not apply to any electronic message specified in the First Schedule to such extent as may be specified therein.

 **Question:** Can an entity in Singapore contribute to the mailing of spam but not get into trouble under the Spam Control Act

PART 2: DICTIONARY ATTACK AND ADDRESS-HARVESTING SOFTWARE

Application of this Part

8.—(1) Subject to subsection (2), this Part applies to all electronic messages, whether or not they are unsolicited commercial electronic messages.

(2) This Part does not apply to any electronic message sent to a mobile telephone number.

Use of dictionary attack and address-harvesting software

9. A person must not send, cause to be sent, or authorise the sending of, an electronic message to electronic addresses generated or obtained through the use of —

- (a) a dictionary attack; or
- (b) address-harvesting software.

just because you obtained it does not mean can spam it

PART 3: UNSOLICITED COMMERCIAL ELECTRONIC MESSAGES

Application of this Part

10. This Part applies only to unsolicited commercial electronic messages.

Sender of unsolicited commercial electronic messages in bulk to comply with Second Schedule

11. Any person who sends, causes to be sent or authorises the sending of unsolicited commercial electronic messages in bulk must comply with the requirements in the **Second Schedule**.

 Companies whose business model is harvesting online information would have to ensure:

1. collection is in regulation with PDPA
2. buyer is not going to spam

AIDING, ABETTING, ETC. NOT ALLOWED

12.—(1) A person must not —

- (a) aid, abet or procure a contravention of section 9 or 11;
- (b) induce, whether by threats, promises or otherwise, a contravention of section 9 or 11;
- (c) be in any way, directly or indirectly, knowingly concerned in or a party to, a contravention of section 9 or 11; or
- (d) conspire with others to effect a contravention of section 9 or 11.

(2) A person does not contravene subsection (1), section 9 or 11 merely because the person —

- (a) provides, or operates facilities for, online services or network access; or
- (b) provides services relating to, or provides connections for, the transmission or routing of data.

CIVIL ACTION

13.—(1) Where there is a contravention of section 9 or 11 in relation to electronic messages sent to electronic addresses, any person who has suffered loss or damage as a direct or an indirect result of that contravention may commence an action in a court against —

- (a) the sender; or
- (b) a person who has contravened section 12(1).

(2) This section does not affect any liability that any person has under any other written law or rule of law.

INJUNCTION AND DAMAGES FOR CIVIL ACTION

14.—(1) Subject to the provisions of this Act, in an action under section 13(1), the types of relief that the court may grant include the following:

- (a) an injunction (subject to any terms that the court thinks fit);
- (b) damages;
- (c) statutory damages under subsection (3).

(2) The types of relief mentioned in paragraphs (b) and (c) of subsection (1) are mutually exclusive.

(3) In any action under section 13(1), the plaintiff is entitled, at the election of the plaintiff, to —

(a) damages in the amount of the loss or damage suffered by the plaintiff as a direct or an indirect result of the contravention mentioned in section 13(1); or

(b) **statutory damages —**

(i) **not exceeding \$25 for each electronic message mentioned in section 13(1); and**

(ii) **not exceeding in the aggregate \$1 million, unless the plaintiff proves that the actual loss suffered by the plaintiff from such electronic messages exceeds \$1 million.**

INJUNCTION AND DAMAGES FOR CIVIL ACTION

- (4) In awarding statutory damages under subsection (3)(b), the court is to have regard to —
- (a) whether the contravention by the defendant of section 9, 11 or 12(1) was wilful;
 - (b) any loss or damage that the plaintiff has suffered or is likely to suffer as a direct or an indirect result of the contravention mentioned in section 13(1);
 - (c) any benefit shown to have accrued to the defendant by reason of the sending of electronic messages;
 - (d) the need to deter other similar instances of sending of electronic messages; and
 - (e) all other relevant matters.
- (5) The loss mentioned in this section includes any pecuniary loss suffered as a direct or an indirect result of the contravention mentioned in section 13(1).

10:00

PRIVACY AND DATA PROTECTION





HOW ARE YOU TRACKED ON THE INTERNET?

- IP addresses
- Geolocation tracking
- Cookies (browser, Flash)
- Keystrokes
- Third party cookies
- Server side session 'cookies'
- Beacons - invisible (or one-pixel GIFs)
- Browser fingerprinting
- Canvas fingerprinting
- Web-cams
- Click-jacking
- Spyware

WHO IS TRACKING YOU?

- Social media sites
- Cell phone companies
- Email services
- Cell phone apps
- Online retailers
- Search engines
- Governments
- Your parents

HOW MUCH INFORMATION DO THE SITES HAVE ABOUT YOU?

- Login information (everything!) (i.e., your cat's name, your date of birth, your favourite colour and your nickname for your bf, gf, etc.)
- Publicly available information (IDs, addresses)
- Relationships (previous employment, friendships)
- Browsing history
- Viewing history (intentional data)
- Purchasing history (affinity data)
- Location

HOW I WANT PEOPLE TO HANDLE MY DATA

- Use the Zoom Poll
- Choices are:
 - A. I'm OK with the government having my data but not private companies
 - B. I'm OK with private companies having my data but not the government
 - C. I am not OK with anyone having access to my data except those to whom I have given explicit consent and only for the purposes to which I have consented
 - D. I'm OK with anyone having access to my data because everyone already has it. Why pretend otherwise.

DATA AS AN ASSET VS. DATA AS A RIGHT

WHY YOU SHOULD CARE ABOUT HOW DATA IS BEING PROCESSED

- What is the information being used for?
- Do they have my consent?
- Who is collecting information about me?
- Whom do they pass the information to?
- Who uses the information?
- What if the information is “abused” ?
- What if a profile is built about me for unfair purposes e.g. discriminatory pricing?
- What if the information is erroneous?
- What if the information is leaked?

DATA AS AN ASSET VS. DATA AS A RIGHT

- How should we classify data? This goes to the heart of understanding the difference between data as a right vs. data as an asset.
 - Trade secrets / confidential information – How do we categorize these?
 - Personal data – How should we categorise these?
 - Insights obtained by analysing personal data – How should we categorize these?

WHAT ARE THE IMPLICATIONS WHEN WE TREAT DATA AS AN ASSET?

- Data as a form of property – well developed body of laws and regulations that govern property
 - Exclusive and Proprietary
 - Right to exploit
 - Can be taxed
 - Can be subject to antitrust regulation

WHAT DOES IT MEAN TO SAY THAT DATA IS A RIGHT?

DEFINING PRIVACY

- Warren and Brandeis, “The Right to Privacy”
 - “the right to be left alone”
 - Intimacy
 - Right of solitude
 - Freedom from interference
- Protection of individual honour or dignity
 - Respect for private and family life
 - Any interference to be necessary in the interests of national security, public safety, economic well-being of country, prevention of disorder or crime, protection of health or morals, protection of the rights and freedom of others (ECHR)
- Societal benefit in insulating private sphere of life from public gaze

WHAT IS DATA PROTECTION

Protection of privacy as extending to regulating activities associated with information characterized as private – “data protection”

- Private data vs. personal data vs. public personal data
- Creation of rights to give an individual “control” over personal data
- Cf. Can data be “controlled”? Does personal data “belong” to an individual?
- Additional humanistic rights associated with regulation of activities e.g., data correction

WHAT IS THE PURPOSE OF PERSONAL DATA PROTECTION

Purpose

3. The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

SECOND READING OF PERSONAL DATA PROTECTION (AMENDMENT) BILL

“... give greater certainty for organisations to use data for legitimate business purposes with the requisite safeguards, and it will ultimately enhance Singapore’s status as an important node in the global network of data flows and digital transaction.”

- Minister for Communications and Information (Mr S Iswaran)

A BALANCING ACT?

- Is “data protection” a balancing exercise? How is this balance reached? Who does this balance favour? Who is this “reasonable person”?

BALANCING EXERCISE POINT 1: RIGHT VS. ASSET

- PDPA improves Singapore's competitiveness as a business destination to “promote business innovation and enhance competitiveness”
- PDPA as enacted “can lead to better services and products that help local businesses become more competitive”
- PDPA to make Singapore a “global data hub by providing a conducive environment for global data management industries, such as cloud computing and business analytics, to operate in Singapore” and “enhance Singapore's status as an important node in the global network of data flows and digital transaction.”
- Question: What about the “individual” in “personal data”?

BALANCING EXERCISE: POINT 2: DATA PROTECTION VS. INFORMATION SECURITY

- both concepts are consistent *and* contradictory
- from perspective of company and data subject
 - “integrity” to guard against improper information modification or destruction – yet individuals have rights to **modify and seek destruction of information about themselves**
 - “confidentiality” to preserve authorized restrictions on access and disclosure – yet companies “share” personal data with other companies for commercialization purposes
 - “availability” to ensure timely and reliable access to and use of information – yet individuals also want to deny companies access to their personal data

CONCEPT OF LEX INFERIORI

Unless otherwise expressly provided in this Act —

- (a) nothing in Parts 3, 4, 5, 6, 6A and 6B affects any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation is not an excuse for contravening this Act; and
- (b) the provisions of other written law prevail to the extent that any provision of Parts 3, 4, 5, 6, 6A and 6B is inconsistent with the provisions of that other written law.