NATIONAL UNIVERSITY OF SINGAPORE

IFS 4101 – LEGAL ASPECTS OF INFORMATION SECURITY

AY2021/2022, Semester 2, Week 10

LAWS AFFECTING E-COMMERCE AND PERSONAL DATA PROTECTION

REQUIRED READINGS FOR THE TOPIC

1. *Second Reading, Electronic Transactions Bill*, Official reports – Parliamentary Debates (Hansard), Jun. 29, 1998, col. 251 *et seq*.
2. Electronic Transactions Act 2010 (especially Parts 1, 2, 4 and 4 and First Schedule)
3. *Metupalle Vasanthan and another v Loganathan Ravishankar and another*, [2021] SGHC 238 (https://www.elitigation.sg/gdviewer/s/2021_SGHC_238)
4. *Second Reading, Spam Control Bill*, Official reports – Parliamentary Debates (Hansard), Apr. 12, 2007, col. 568 *et seq*.
5. Spam Control Act 2007
6. *Simon Chesterman, After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore's Personal Data Protection Act 2012*, [2012] SJLS 391 (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2042144)
7. Personal Data Protection Act 2012 (Part 1 and Part 3)

I. INTRODUCTION

Many laws regulate commerce in general, but here are some that are critical to e-commerce:

- Electronic Transactions Act
- Spam Control Act 2007
- Personal Data Protection Act 2012

II. ELECTRONIC TRANSACTIONS ACT 2010

We take for granted these days that we can conduct e-commerce online and that all those online transactions would be enforceable in court if there were a dispute. This was not always the case.

Unlike the offline world where the process for formation of contracts is very clear, that was not the case back in 1998 when the first version of the Electronic Transactions Bill was mooted. In the physical world, people signing contracts could affix their signatures onto paper. The copies of the paper were then exchanged so that each side to the contract would receive one fully-executed copy of the contract with everyone's signature on it. Critically, the signing process could be witnessed by others who would also affix their signatures (as witnesses) onto the contract. In the event of a dispute, one could call on the witnesses to attest and authenticate the signatures on the contract as representing the intent of the signer to be bound.

In the case of electronic signatures, how do we ensure that the signer intended to be bound by the terms of the contract? How do we authenticate the signatures and get assurances that the electronic signing was not forged? How do we ensure that the "sign-off" on a transaction provided through account was submitted by the owner of the account and not someone else? How do we guard against people who authorise the electronic transaction but later try to disavow the transaction by claiming that the entire signing activity was done by someone else who hacked into the account?

Furthermore, the contract terms of electronic changes change all the time. Anyone who has ever transacted electronically knows that the terms of service posted on the e-commerce site changes frequently. And none of us bothers to download the terms of service at the time that we transact with the e-commerce merchants. When a dispute arises, how does the consumer get access to the contract terms that existed at the time of signing the contract? Is it fair to the consumer to be forced to accept changes to the terms of the contract that merchants implement after the transaction was consummated?

The Electronic Transactions Act ("ETA") was adopted to resolve most of these questions and to enable the transition of Singapore's public agencies into provision of digital services (see Part 5 which empowers any Singapore public agency to accept electronic filings, issue electronic licenses and make payments in electronic forms).

The ETA owes its parentage to the Utah Digital Signature Act 1995, the world's first digital signature legislation, and the Model Law on Electronic Commerce 1996 (Model Law) adopted by the United Nations Commission on International Trade Law. It has since been amended a few times to bring the law into harmony with other global standards.

A. Giving Weight and Legal Status Allow Electronic Records to be Used to Document Contracts

What were the key changes brought about by the ETA? They can be found in Sections 6, 7, 8 and 11(1).

Section 6 of the ETA took away the concern that businesses had over whether electronic transactions concluded using an electronic record could be recognised in court by declaring that: "*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.*" Section 11(1) further provided that where the formation of contracts is concerned, the general rule is that offers and acceptances can be expressed electronically.

Section 7 endowed upon electronic records the functional equivalence of "writing" as understood in the law, which meant that under other types of legislation that required something to be "writing", the use of an e-mail, for example, would be able to satisfy that "writing" requirement. This small change has consequential effect, including as an example, converting the legal character of the defamatory content contained in an e-mail from that of slander to that of libel. Section 8 also stated that where a rule of law required a signature, that requirement can be satisfied by some method that can be used to identify the person whose signature is required. Read *Metupalle Vasanthan and another v Loganathan Ravishankar and another*, [2021] SGHC 238 for an example of what fails to constitute a signature that is recognised by the ETA.

Why were these changes needed? Historically, the common law required transactions that exceed a particular value to be in writing to reduce the chance of fraudulent claims about a contract's existence or its terms (known as the "Statute of Frauds"). Moreover, because of the difficult inherent in identifying the actual signatory of

a piece of electronic content, from an evidentiary perspective, the burden of proving the authenticity (and admissibility) of an electronic record and the existence of a contract documented by that electronic record would lie on the party trying to assert a breach of contract claim. However, that makes it very difficult for anyone to try to prove the existence of a contract that is documented electronically because the claimant would have to first establish that the systems used to establish the electronic record is reliable, accurate, etc.

Between Sections 6, 7, 8 and 11(1), the ETA made it possible for litigants to file actions to enforce contracts that are documented using electronic records by relying on legislation that required the courts to presume the validity of the electronically formed contracts. These changes, therefore, made the use of electronic contracting reliable enough for use to document commercial and other types of transactions.

B. Resolving Ambiguities of Electronic Transactions

What are the other issues of electronic transactions resolved by the ETA? In any electronic transactions, these questions always arise:

- When and where was the contract signed?
- Does posting information about a product or service online constitute an offer to sell that product or service?
- Can automated messages be used to enter into contracts?
- What about errors in communications? What if I pressed the "buy" button by mistake?

1. Time and Place of Contracting

While the time of contract signing is easy to determine in the physical world, it is less certain in the digital world. Let's take email as an example. An email written and sent out by the sender will first be sent from the desktop client to the mail server on the network. The email is then processed by the mail server to be sent out to the recipient's email address in the form of electronic packets. When it arrives at the recipient's email server, it resides on the server until it is accessed. This being the case, when is the actual moment of despatch or receipt of electronic mail or electronic records? Should the contract be deemed to be signed at the moment of despatch or the moment of receipt?

Then, there is the question of the location where the contract is signed. Businesses need to know the answer because the place of signing of a contract frequently will have tax implications and may even affect where a lawsuit can be initiated. But in the world of electronic transactions, especially where cross-border transactions are involved, how do we determine the actual location in which the contract was signed. Was it at the seller's location? Or the Buyer's location? Or the location of the email server and, if so, whose server?

Read Section 13 of the ETA for answers to these questions.

2. Online Stores as Soliciting Offers

Traditionally, advertisements are not deemed to constitute offers to sell a product or service because the typical advertisement is too general and contains too little information to make it reasonable for anyone to view it as an offer. However, e-commerce stores are very different when compared to offline stores. In the e-commerce world, merchants go out of their way to describe their products in great detail, giving out the product specifications, the price, promises of deliveries, amount of stock available and

even ways to secure delivery timelines. The more detailed these descriptions get, the more the information looks like an offer to sell a product or services, as understood in common law precedents.

Why does this matter? If the product listing and descriptions constitute an offer to sell, then, when a buyer accepts that offer, a contract is formed. At that point in time, the seller must fulfil the terms of the contract. A seller who delays the delivery of the product or has run out of the product to sell cannot postpone delivery or cancel the order as doing either would constitute a breach of contract, which would entitle the buyer to various contractual remedies, including the remedy of buying alternative products at a higher cost from a different vendor and requiring the seller who breached the contract to reimburse the buyer for the additional amount the buyer had to pay to get the alternative goods.

Recognising this to be a potential problem, Section 14 of the ETA clarified that the listing of products for sale on an e-commerce store is viewed as an invitation to make an offer, and not an offer.

3. Automated Messages for Concluding Contracts

One of the most attractive aspects of e-commerce is that businesses are running 24/7 – 24 hours a day 7 days a week – as many of the business transactions are now highly automated at a relatively low cost. While the computer is able to deliver emails seamlessly without human intervention, it was once doubtful if information systems were able to legally contract.

Section 15 of the ETA resolves that issue by stating that just because an offer to buy a product was accepted through the means of an automated order confirmation, it does not mean that the automated acceptance can be denied validity or enforceability at first glance.

4. Error in Electric Communications

What happens when a customer accidentally presses the "Buy" button by mistake? In a traditional contract setting, a person who accidentally signs a contract can simply shred the document and pretend that the signing never took place. In an electronic environment, once a customer clicks on the trigger that records the customer's detail, an electronic record is created recording the customer's intent to consummate a transaction.

Section 16 of the ETA was adopted to allow the withdrawal of the portion of the electronic communication in which the input error was made as long as prompt notice is given and the person seeking to withdraw has not benefitted from the value of the goods and services. While this section helps those who buy consumer goods and services withdraw from contracts that were mistakenly entered into, it is not clear that this section can be relied upon to withdraw from transactions involving the trading of securities as many financial products change hands instantaneously.

C. Presumption Given to Accuracy and Reliability of Secure Electronic Records and Signatures

If a party introduces a secure electronic record or secure electronic signature into evidence, Part III of the ETA places the burden of proof of disproving the authenticity, accuracy and reliability of a secure electronic record and secure electronic signature on the other party to challenge the record and signature.

D. Excluding Certain Legal Instruments from the ETA

As the parliamentary debates explained, in adopting the ETA, there were concerns that certain types of legal instruments requiring signatures that should continue to require signatures that are signed using ink. As a result, Section 4 of the ETA specifically excluded certain instruments from the benefits provided under the ETA. The list of excluded instruments was incorporated into the First Schedule of the ETA.

In March 2021, an amendment to the ETA was enacted that resulted in the removal of one category of instruments: *Negotiable instruments, documents of title, bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money*. These are instruments that are critical to trade (and especially the maritime industry) and it is envisioned that allowing them to be subject to the ETA will speed up the entire logistics chain. The expansion of the ETA to cover these instruments (defined as "electronic transferable records") also opens up business opportunities to develop electronic transferable records management systems that are accredited so that transactions carried out through these systems are presumed to be reliable and to qualify for the benefits of the ETA.

E. Information Security and the ETA

Why does the IS professional care about the ETA?

The ETA is a very powerful tool that businesses can use to speed up business transactions. However, the ETA is only powerful as a tool if systems have been set up for creating electronic records in a manner that can be reliably used as evidence of transactions. In particular, IS professionals need to understand the conditions under Sections 7, 8 and 9 of the ETA that must be satisfied in order for electronic records to be afforded the benefits that the ETA provides.

As an example, Section 7 allows electronic records to satisfy the "writing" requirement under a rule of law only if the electronic record is accessible so as to be usable for subsequent reference. This means that there must be a way to store that electronic record that allows for it to be accessed in the future, and that the storage manner must allow this data to be usable in the future. This means that as older technology is deprecated, we need to ensure that the newer hardware is backward compatible so that it can continue to access the electronic records created by older technologies, or, alternatively, the IT department must continue to maintain older hardware so that the electronic record created using older technology continue to be accessible.

Section 8 allows electronic signatures to be used where there is an established method used to identify the signatory and to indicate that signatory's intent. Therefore, the IS and Legal teams must work together to understand how to create a process of documenting the intent of the signatory and keeping a record of that intent in a manner that meets the requirements of Section 8.

Read Section 9 of the ETA to understand the requirements that must be met for using electronic records to retain documents in compliance of laws that require the retention of documents (e.g., tax laws requiring companies to retain copies of invoices, etc.). Read Section 19 of the ETA to understand the conditions under which "originals" of documents can be retained in electronic form.

III. SPAM CONTROL ACT 2007

E-commerce, as with all commerce, runs on advertisements. The major difference is that digital advertising is a lot cheaper, and, therefore, much more scalable. Unfortunately, such scalability also means an unprecedented level of intrusion that is directed towards consumers. One of the biggest means of intrusion is the spam (i.e., unsolicited commercial communications sent in bulk by email, SMS or MMS).

A. Requirement for a Singapore Link

Section 7 of the Spam Control Act ("SCA") limits the applicability of the SCA to those that meet the "Singapore link" definition.

Question: Can you think of a service provider in Singapore who may play a part in sending spam and is located in Singapore but will not be subject to liability under the SCA? Consider whether such a provider could be liable under Section 12 for aiding and abetting the contravention of Section 9 or 11 of the SCA.

B. Regulation Mainly Aimed at the Form of the Communications

Part 3 of the SCA aims to regulate the form of the communications to allow the recipients of electronic messages to identify the sender and to have a mechanism for unsubscribing from future communications.

Question: Identify the different types of marketing communications are subject to regulation under the SCA.

Contrast the SCA which regulates the form that the communications have to take versus the "Do Not Call" ("DNC") provisions of the Personal Data Protection Act 2021, which provides for the development of a registry. Under the DNC regime, consumers can register their telephone numbers and specifically opt out of receiving unsolicited calls, text messages and/or fax. Telemarketers are required to cross check their list of targets against DNC registry before conducting telemarketing activities. There is no equivalent registry for e-mail addresses.

C. Regulation Aimed at Communications

Part 2 of the SCA also regulates the sending of spam using target addresses collected by dictionary attacks and address harvesting software.

Question: Why doesn't the SCA regulate the development or use of address harvesting software itself or dictionary attacks? Why should the regulation be limited to the sending of electronic messages to electronic addresses generated by these methods?

D. Civil Liability

Section 13 of the SCA authorises civil action to be taken against those found in breach of the SCA. Section 14 of the SCA sets out the types of damages that can be recovered. Pay attention in particular to the ability to assess statutory damages of up to $25 for each electronic message found in violation of Section 9 or 11 of the SCA.

Question: Why do you think it is necessary to establish statutory damages?

IV. PERSONAL DATA PROTECTION ACT 2012

For this class, we will be examining the topic of data protection, from the perspective of information security. As this can only be done with some background into data protection, much of the seminar will be about the Singapore Personal Data Protection Act or PDPA. However, the focus will be on identifying how data protection issues will raise information security issues, and how a proper application of information security considerations can address or ameliorate these issues.

In the modern knowledge economy, companies use personal information about their individual customers to allow them to provide better goods and services to their customers, to manage their staff more efficiently and to compete more effectively in the marketplace. The amount of information that companies retain about individuals is enormous, yet many individuals seem to be either unaware about the fact that companies have personal data about them, let alone the extent to which data is collected about them. Concerns have been raised that left unchecked, companies may misuse and abuse this data. In addition, the unauthorised disclosure of such data by third parties, and its possible compromise by hackers and criminal elements, may have the potential to create identity, authentication, social and economic problems for individuals as well as the companies who use such data. In the light of these concerns, the Singapore Personal Data Protection Act 2012 ("PDPA") was passed. While Singapore previously had piecemeal legislation to deal with certain elements data protection elements in specific contexts such as health and banking, the enactment of the PDPA was the first omnibus legislation in Singapore to attempt to address the issues of data protection across all organisations and industries, and in all contexts.

A. Concept of Privacy vs. Data Protection

Before we talk about personal data protection, however, we need to first understand the difference between the concepts of privacy and data protection. Data protection and privacy are two separate rights. However, these two rights are inextricably interlinked in many jurisdictions, especially in the European Union region.

The notion of privacy is strongest in the United States and in the EU region and it is also enshrined in the Universal Declaration of Human Rights (Article 12). In the US, the notion of privacy historically has often been regarded as an element of liberty, the right to be free from intrusions by the state.

In the EU, human dignity is recognised as an absolute fundamental right and the notion of human dignity requires that individuals have agency and control over the information about themselves. Therefore, privacy is but one aspect of what it means to have human dignity. The EU also believes that privacy is not merely an individual right but also has social value and has enshrined the right to privacy in the European Charter of Fundamental Rights (Article 7).

In Singapore, there is no express right of privacy under the Constitution and a constitutional right to privacy implied in the Constitution has been so far rejected.[1]

B. What is Data Protection?

Unlike privacy which is tied to the notion of personal autonomy and human dignity, data protection is a more practical form of right. It is about protecting any information

[1] *Lim Meng Suang v Attorney-General* (2015) 1 SLR 26 (CA).

relating to an identified or identifiable natural (living) person, including names, dates of birth, photographs, video footage, email addresses and telephone numbers, from use that was never anticipated by the individual involved, or the data subject.

In the EU, the notion of data protection originates from the right to privacy. The EU takes the position that the rights to privacy and data protection are both are instrumental in preserving and promoting fundamental values and rights; and to exercise other rights and freedoms - such as free speech or the right to assembly. Contrast this with the position in the United States, which traditionally has taken the position that information should be free flowing and any restrictions on information flow and regulation by government should be treated with suspicion as a potential violation of the First Amendment.

The Organisation for Economic Co-operation and Development ("OECD") took the lead in formulating what was the first set of principles for the protection of personal data in a globalised setting. The impetus behind the OECD's work was to address the growing transborder data flows and the need to find a way to bridge the different philosophies between the United States' treatment of data and the European philosophies. There was a recognition that with the growth of automated data processing, some form of controls must be implemented to avoid the abuse that would come about through unimpeded data collection, regardless of whether the organisation collecting that information is the private or public sector.[2] The OECD Guidelines form the bedrock of privacy principles upon which almost all data protection laws are built, including the EU's General Data Protection Regulation (GDPR).

C. General Principles of Data Protection

The OECD principles of data protection are given below.

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those

[2] The European concern about the abuse of data collection is driven largely by the Jewish experience with the Holocaust. The Nazis used identity card systems adopted by European nations to track and eliminate resistance fighters and Jews. In countries that had implemented systems that were hard to counterfeit, very few Jews and resistance fighters survived. In contrast, the Nazis had a harder time tracking down their enemies in countries that had systems that were less secure. This background is critical to understanding why Europeans are, in general, much more protective over how their personal data is to be used when compared to nations that have not suffered a similar experience.

purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10 Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time;

at a charge, if any, that is not excessive;

in a reasonable manner; and

in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.