II. NATIONAL E-COMMERCE LEGISLATION IN ASIA AND THE PACIFIC: THE CASE OF SINGAPORE

By Goh Seow Hiong[9]

A. Overview

The e-commerce legal framework of a nation can play an important role in enabling and facilitating e-commerce transactions within the country and across its borders. Such legislation creates the much-needed sense of certainty that for traditional paper-based physical business transactions that are paper-based canto be carried out in the electronic realm.

The foundation behind the formation of electronic contracts and the issues relating to disputes over such transactions need to be examined in order to understand the legal framework for e-commerce in Singapore. This requires a discussion about the present legal framework that provides the rules upon which electronic contracts are formed. There are also evidentiary issues to be discussed in relation to matters of proof when it comes to disputes over electronic transactions. Finally, the question of what is ahead for e-commerce laws in Singapore is considered.

B. Foundation for electronic contracts

Under general contract law, there are well-established principles and rules that deal with how a legally binding contract is created. There must be an intention to create legal relations between the parties concerned, and each party must have the capacity to enter into the contract. There should be an offer made by one party and an acceptance of the offer by the other party, and there should generally be consideration[10] between the parties of the contract. The principle of privity of contract says that only a party to a contract can enforce the contract, even if the contract was for the benefit of a third party. There are, however, exceptions to this

---

[9] Director, Software Policy for Asia, Business Software Alliance <www.bsa.org>. The information provided in this article is not intended to be nor is it a substitute for formal legal advice, but is only intended as a general guide and non-exhaustive discussion of the issues involved. A qualified legal practitioner should be consulted for specific advice in relation to e-commerce transactions and contracts entered into. The law is as stated in June 2004.

[10] Consideration is the legal term given to the need for reciprocity or a bargain in contracts. It is the element of exchange, essentially a benefit to one party or a detriment to the other party.

principle.[11] Finally, the contract must not be contrary to public policy. The application of these rules and principles together determine whether a contract is valid and binding.

In addition, some other concepts apply for electronic contracts. The main legislation in Singapore governing electronic contracts is the Electronic Transactions Act (ETA).[12] While the law of contracts continues to apply broadly to both the physical and electronic world, the ETA fills the gaps where rules governing contracts in the physical world need to be supplemented to deal with the environment enabled by new technologies. The intention is for the ETA to be considered as consistent with commercially reasonable circumstances.[13] The ETA also provides additional legal support for new technologies to assist the court in recognizing electronic evidence.

The ETA was passed in 1998 as enabling legislation to remove uncertainty about the legality of contracts formed electronically, to recognize electronic signatures and to clarify the liability of network service providers who only carry electronic traffic. The ETA sets out the voluntary licensing of certification authorities (CAs)[14] as trusted third parties in the online world to provide the basis for establishing other trust relations.

The Electronic Transactions (Certification Authority) Regulations[15] stipulate the requirements for a CA to obtain a licence in Singapore. The accompanying Security Guidelines for Certification Authorities[16] stipulate the technical security requirements that must be met. The ETA also has provisions that enable Government agencies to implement electronic systems easily in order to transact with the public without the need to amend their own governing acts. The ETA provides for the acceptance of applications and issuance of digital licences, with the ability to send and receive electronic documents in a reliable manner.

---

11 Contract (Rights of Third Parties) Act (Singapore), Rev. Ed. 2002, Chapter 53B.

12 Electronic Transactions Act (Singapore), Rev. Ed. 1999, Chapter 88 http://www.cca.gov.sg (Cited hereafter as ETA.)

13 Section 3, ETA.

14 Technological solutions are available, if used, to prove to third parties the identity of the sender of an electronic message and to protect the integrity of such messages.

15 Electronic Transactions (Certification Authority) Regulations (Singapore), Rev. Ed. 2001, Regulation 1 <http://www.cca.gov.sg>.

16 Security Guidelines for CAs, September 1999 <http://www.cca.gov.sg>.

C. Electronic records, signatures and contracts

Some specific ETA provisions related to electronic records, signatures and contracts as well as their secure counterparts should be examined in further detail. The ETA gives electronic documents and records the same legal standing as physical documents by declaring that the validity or enforceability of such electronic versions cannot be denied their legal effect on the basis of being electronic.[17] The ETA makes it clear that where a rule of law requires information to be in writing, an electronic record containing that information will also satisfy the requirement, as long as the information can be accessed for subsequent use.[18] Similarly, where a rule of law requires a signature, an electronic signature will also satisfy the rule of law.[19] The ETA provides that an electronic signature can be proven in any manner.[20]

Where there are legal rules governing the retention of documents and records, the ETA sets out the circumstances and requirements for satisfying such rules by storing the information in electronic form.[21] However, where the rule of law already expressly requires electronic records to be retained, or where a government agency or organ of state has stipulated additional requirements, such requirements must be followed.[22] In addition, where the notice provision in a contract specifies the means (such as post or facsimile) to notify another party in writing, if e-mail or other electronic means are not explicitly listed as authorized means of notification, then electronic means may not be accepted as a valid method of giving notice.

The ETA expressly states that contracts can be formed electronically, unless the parties have agreed otherwise.[23] Any offer and acceptance for a contract can be made in the form of electronic records or messages. The intention of the parties when entering into a contract conveyed in electronic form is of equal standing as that conveyed through traditional means.[24] Attribution refers to how the identity of the originator and the addressee of an electronic record will be determined, and the ETA

17 Section 6, ETA.

18 Section 7, ETA.

19 Section 8(1), ETA.

20 Section 8(2), ETA.

21 Section 9, ETA.

22 Section 9(4), ETA.

23 Section 11, ETA.

24 Section 12, ETA.

has provisions governing this matter.[25] The parties can also agree on an acknowledgement of receipt for electronic records to be sent by the recipient. The ETA provides that the receipt of the electronic record can be conditional upon the receipt of the related acknowledgement.[26] Receipt of such an acknowledgement can only be used to presume that the related electronic record was received, but not that the content of the sent record corresponds to the content that was received.[27]

The ETA also deals with other important elements in the formation of contracts. These include the time and place of despatch and receipt of the electronic records relating to the contract. There may be explicit agreement between the parties, or in some circumstances, may be prescribed through regulations. In the absence of such stated or explicit circumstances, the despatch of a record occurs when it enters a system outside the control of the originator.[28] In practical terms, if a party is using a personal computer in the course of forming an electronic contract by e-mail, despatch occurs when the message sent by that party leaves his computer and enters another machine outside his control (for example, the Internet service provider).

On the receiving side, the timing for receipt depends on whether the recipient has designated a particular system to receive such records. If there is a designated system, the time of receipt is when the record enters that designated system. The time of receipt for a record sent to any other non-designated system is when the record is retrieved by the recipient from the non-designated system.[29] If no system is designated, then the time of receipt is when the record enters a system of the addressee. It is therefore advantageous for an addressee to designate the information system to which such electronic records are to be sent. The addressee will need to check the designated information system with diligence for new records (similar to the need to check for incoming facsimiles). However, records sent to any other non-designated system would be deemed received only when the addressee retrieves the records from such a system.

In the electronic environment, despatch and receipt can take place almost anywhere geographically with a suitable telecommunications link. Hence, the ETA seeks to avoid ambiguity and has deemed the place of business of the originator and

25 Section 13, ETA.

26 Section 14, ETA.

27 Section 14(5), ETA.

28 Section 15(1), ETA.

29 Section 15(2), ETA.

the addressee to be the place of despatch and receipt, irrespective of where the record was actually despatched or received.[30] In cases where there is no such place of business, it will be deemed as the usual place of residence.[31]

The ETA has also allowed parties in a transaction to vary any of the above general rules on electronic contracting by agreement.[32] However, the ETA provides for exceptions when the general rules on electronic contracting mentioned above would not apply.[33] The exceptions include: (a) the creation or execution of a will; (b) negotiable instruments; (c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts; (d) any contract for the sale or other disposition of immovable property, or any interest in such property; (e) the conveyance of immovable property or the transfer of any interest in immovable property; and (f) documents of title. However, these exceptions may be modified by a ministerial order.

D. Electronic signatures and digital signatures, secure electronic records and signatures

The ETA defines an electronic signature as any letters, characters, numbers or other symbols in a digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record.[34] This wide definition includes digital watermarking, scanned images of handwritten signatures, digital signatures and biometric signatures as possible forms of electronic signature. Each type of electronic signature has a different level of security afforded to it.

The ETA further defines a digital signature as an electronic signature that can transform an electronic record by using an asymmetric cryptosystem and a hash function. The signature is such that a person who has the initial untransformed electronic record and the signer's public key can accurately determine (a) whether the transformation was created using the private key that corresponds to the signer's public key and (b) whether the initial electronic record has been altered since the transformation was made.[35]

30 Section 15(4), ETA.

31 Section 15(5), ETA.

32 Section 5, ETA.

33 Section 4, ETA.

34 Section 2, ETA.

35 Section 2, ETA.

Tools such as digital signatures allow for a signature (consisting of a string of numbers) to be attached to a document and provide two essential properties if the signature is successfully verified. First, it confirms that a document has not been tampered with since the time the signature was fixed, and second, it identifies the person who fixed the signature. These features of authentication and non-repudiation are not readily available with handwritten signatures. One means to create and verify digital signatures is through "public key encryption" or "asymmetric key encryption" technology. This involves the use of two distinct keys. They are mathematically related and randomly generated from prime numbers. The first key is known as a "private key". It is held and kept as a secret by the individual making the signature. The second key is a "public key", which can be known to the world-at-large. A public key infrastructure facilitates the use of digital signatures. Under this infrastructure, a Certification Authority (CA) certifies (in the form of a digital certificate) that a given public key is associated with a specific individual. A CA may verify with the individual face-to-face before such a certification is given. The digital certificate can subsequently be used to confirm the public key of an individual and verify the signature generated by the individual. It is essential for the verifier of a signature to know that he is using the correct public key of the individual for verification. It is envisioned that the digital signature would be one of several technologies that could be implemented to secure an electronic signature. The ETA allows for other forms of electronic signatures to be recognized as well.

The ETA further provides for secure electronic records and secure electronic signatures, and the presumptions accorded to such secure forms. A secure electronic record is one that applies a prescribed security procedure or a commercially reasonable security procedure (agreed to by the parties involved) with the capability to verify that the electronic record has not been altered since a specific point in time.[36] If a prescribed security procedure or a commercially reasonable security procedure agreed to by the parties involved is applied, an electronic signature can be deemed secure. The security procedure should be able to verify that at the time the signature was made, it was (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 in such a manner to the related electronic record that if the record were changed, then the electronic signature would be invalidated.[37]

---

[36] Section 16, ETA.

[37] Section 17, ETA.

One important feature of the ETA provides for several presumptions related to secure electronic records and secure electronic signatures that are appropriately verified.[38] The following presumptions are provided, but they can be rebutted: (a) the secure electronic record has not been altered since the specific point in time to which the secure status relates; (b) the secure electronic signature is that of the person to whom it correlates; and (c) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

The ETA further provides for the effect of digital signatures. It specifies how a digital signature will be treated as a secure electronic signature[39] and how an electronic record signed with such a digital signature will be treated as a secure electronic signature.[40] Likewise, the evidentiary presumptions described above will apply in those instances where the associated CA is licensed.[41] In addition, the ETA describes the general duties relating to digital signatures, duties of CAs, duties of subscribers, and the regulation of CAs.[42]

Since there is no prior face-to-face contact between the parties, the services of a CA are useful in relation to e-commerce transactions, because the transactions will be legally binding. Such technology is especially useful when online transactions are of high value or where the identity of the customer is of primary concern. The CA also bears some liability in the event that the CA does not correctly identify the customer.

E. Evidentiary issues of electronic transactions

One basic feature of information systems from which legal issues arise is the alterability of the documents and records. Systems built on e-commerce solutions are no exception. This feature makes the nature of the information and documents stored electronically fundamentally different from their physical counterparts. Unlike physical documents, changes made to electronic documents, if not protected by additional measures, are virtually undetectable. Inevitably, in the event of a dispute

38 Section 18, ETA.

39 Section 20, ETA.

40 Section 19, ETA.

41 Licensing of CAs under the ETA is voluntary.

42 Sections 23-26, ETA for digital signatures; Section 27-35 for duties of CAs; Section 36-40 for duties of subscribers; and Section 41-46 for regulation of CAs.

where such electronic documents need to be produced in court proceedings, challenges would be raised about the reliability and admissibility of the documents.

In Singapore, the Evidence Act (EA)[43] was amended in 1995 to deal with the general admissibility of computer output as evidence. The Evidence (Computer Output) Regulations[44] were promulgated in 1996 to establish the criteria for certifying imaging systems that can archive documents in an electronic form to be recognized under the EA. The amendments provide for the admissibility and weight of computer output to be used as evidence in criminal and civil proceedings, and allow for the accurate reproduction of documents by electronic or other technical processes to be admissible as secondary evidence.

There are three ways to admit computer evidence. The first is by express agreement between the parties in the proceedings that the authenticity and accuracy of the contents are not disputed.[45] This method requires both parties in the proceedings to agree that the computer output should be admitted as it is. This agreement can occur at any time, either before or during the proceedings. The second way is by showing that an approved process was used to produce the computer output.[46] A process is approved when it has been audited and certified by an agency that has been appointed by the Ministry of Law to be a Certifying Authority.[47] The Certifying Authority will audit the process in accordance with the published compliance criteria in order to certify it. Once the process is certified and approved, the presumption under the law is that the computer output produced by the approved process is accurate, unless it is proven otherwise.

The regulations on compliance criteria for imaging systems were published as the First Schedule of the 1996 Regulations. The criteria in the regulations establish how businesses can seek certification and approval for their imaging systems so that they can be used to transform physical documents into electronic form, discard the physical copies and rely on the electronic copies.[48]

---

43 Evidence Act (Singapore), Rev. Ed. 1997, Chapter 97.

44 Evidence (Computer Output) Regulations (Singapore), Rev. Ed. 1997, Regulation 1.

45 Section 35(1)(a), EA.

46 Section 35(1)(b), EA.

47 To be distinguished from a Certification Authority under the ETA.

48 The Auditor-General was appointed as a Certifying Authority under the 1996 Regulations, primarily for the purposes of auditing government systems. In addition, the Ministry of Law, through the Appointment of Certification Authorities notification (Appointment of Certification Authorities (Singapore), Rev. Ed. 1997, S 273/2001), also appointed several other commercial organizations as Certifying Authorities for the private sector. These appointments are renewable for fixed terms.

The third way is by showing that the computer output was generated by a computer that was at all material times operating properly.[49] The party tendering the output will have to prove the accuracy of the computer output to the court. The system operator, manager or other experts may tender evidence to certify that the computer producing the output was operating properly and the computer output is correct and reliable. There should be no reasonable ground to believe that the electronic record is inaccurate, untruthful or unreliable. If there was any malfunction in the system, it should be shown that the malfunction was immaterial. The accuracy of the output cannot be presumed, but needs to be proven, and this is unlike the situation for the approved process.

Additional provisions supplement and support the three methods enumerated above. The EA provides that if the court is not satisfied with the evidence given according to the three methods mentioned, then it may call for further evidence.[50] This provision allows the court to satisfy itself about the accuracy of the output from (a) a person responsible for the operation or management of the Certifying Authority; (b) a person responsible for the operation of the computer; (c) a person who had control or access to any relevant records and facts relating to the production of the computer output; or (d) an expert appointed or accepted by the court.

In ascertaining the legal weight given to the computer output that is to be admitted, the court will consider the following factors:[51] (a) the circumstances from which any inference can be reasonably drawn as to the accuracy of the output; (b) whether the information in the electronic record was recorded contemporaneously with the facts dealt with in that information; and (c) whether any persons involved had any incentive or motive to conceal or misrepresent the information in question.

With the first method of express agreement, in practice, if a dispute has arisen and the point of contention concerns the accuracy of the records, agreement is unlikely to be reached. As such, it is useful to have a prior agreement before the dispute arises (for example, at the time of making the contract) that the computer output will be accepted.

---

49 Section 35(1)(c), EA.

50 Section 36(1), EA.

51 Section 36(4), EA.

Approved process is the second method, which has the advantage in that once a system owner has the system certified and approved, system records stored and produced as computer output in that system will be presumed accurate. The burden would be on the disputing party to prove otherwise. This gives a strong advantage to the system owner and it can be a great burden for the other party without access or knowledge of the system in question to challenge the presumption.

Fallback provision is the third method, where in the absence of any agreement or the use of an approved process, it is left to the parties to prove the reliability of the output. Once proven, the electronic document may then be admitted as evidence.

For e-commerce systems, the EA and ETA offer two avenues through which the records of e-commerce transactions can be proven in court in the event of a dispute. The appropriate framework to be adopted for any specific system depends on the particular characteristics of the technical system in use and the nature and the manner in which the transaction is conducted. The two approaches offer flexibility for the parties to choose an approach solution that best meets the business and legal requirements while balancing the security and usability requirements of the transaction.

F. Looking ahead

The Singapore Government has called for a public consultation to review the country's cyber legislation. The scope of the review includes the ETA and the Electronic Transactions (Certification Authority) Regulations. The objective of the review is to update and fine tune the legislation and regulations to address the changing environment and international developments since the original enactment was made about five years ago. It is expected that changes to the law would be made by the first quarter of 2005.

There are three stages to the public consultation, which is done through consultation papers issued by the Infocomm Development Authority of Singapore and the Attorney-General's Chambers.[52] The first stage would deal with electronic contracting issues. The second stage would deal with areas of exclusions under the legislation, and the third stage would deal with electronic signatures and certification authorities. Consultation papers on the first two stages of the consultation have been released so far.

[52] Available at http://www.ida.gov.sg and http://www.agc.gov.sg

In the first part of the consultation dealing with issues of electronic contracting in the ETA, feedback was sought on six broad areas. The first area is in relation to party autonomy. The issues under consideration are whether the law should compel parties to accept offers and acceptances in electronic form and whether there should be certain mandatory requirements in electronic contracting that are not open to variation by the parties.

The second area is about the recognition of electronic signatures. The issue being considered is whether the UNCITRAL requirements in relation to function and reliability are consistent with the current provisions under the law. The third area is about the formation of contracts. The issues under consideration include whether there should be a provision relating to when the offer and acceptance made in the electronic world should take effect, and whether a proposal to enter into an electronic contract made to the world-at-large should be considered an invitation to make an offer.

The fourth area concerns the rules on time and place of despatch and receipt. The issue under review is whether the present rules should be amended to be consistent with UNCITRAL relating to the control over the electronic message and the capability to retrieve messages rather than the information system being used.

The fifth area is in relation to automated systems. The issue involves consideration of the status of electronic contracts resulting from the interaction with automated systems, as well as issues relating to errors made by a person in communication with an automated system.

The sixth area focuses on miscellaneous issues, such as the validity of incorporating terms and conditions by reference in electronic communication, the manner in which the originality of an electronic document is to be addressed, and whether legislation relating to the sale of goods in the physical world applies to electronic goods.

The second part of the consultation on the exclusions under Section 4 of the ETA considers the rationale behind the exclusions. Feedback has been sought on whether the exclusions should be retained or modified. The recommendations in the consultation paper are that no changes be made with respect to wills, negotiable instruments and documents of title. In addition, the following instruments are considered:

(1) For indentures, it is recommended that secure electronic signatures may be allowed to satisfy the requirements of sealing a deed.

(2) For trusts, the proposal is to limit the exclusion only to testamentary trusts and trusts relating to land.

(3) For power of attorney, the consultation paper observed that there are benefits to removing the exclusion, although some jurisdictions limit the exclusion to certain types of powers of attorney.

(4) For transfer of immovable property, instead of a wide exclusion, consideration is being given to whether certain classes of people or types of land transactions should be allowed.

(5) For carriage of goods (including documents of title and negotiable instruments), feedback is sought on whether it should be permitted in a manner consistent with the UNCITRAL Model Law on Electronic Commerce.

The consultation process would also welcome any other feedback on additions or amendments to the exclusions presently provided under Section 4 of the ETA. The consultation period for the first stage has already concluded and the second stage was scheduled to close in August-September 2004.