REGULATING THE USE OF ELECTRONIC SIGNATURES GIVEN THE CHANGING FACE OF CONTRACTS

NAZZAL M. KISSWANI* AND ANAS A. AL-BAKRI**

Signatures have always been important in contracts; the nature of contracts is changing due to the internet and the introduction of new technologies in the commercial world. In response, technology has also been changing to maintain the importance of signatures in contract law. This paper outlines the development in the law domestically and internationally in regulating the use of electronic signatures given the changing face of contracts and its influence on electronic commerce.

I INTRODUCTION

The internet has become an everyday reality for many of us. New words have entered our life: cyberspace, dot-com, e-mail, and e-commerce. In terms of electronic commerce which refers to transactions conducted via electronic media, historically such transactions were required by law to be in writing or signed to ensure the availability of reliable evidence that the parties to the transaction intended to proceed with transaction. Electronic commerce has expanded from a limited range of business to business transactions between parties, to a very wide range of different activities involving parties who may not know each other and have never met face to face. Among these, businesses involved in international transactions should be aware of electronic signatures. Many countries such as Australia, the United States, Germany and China have introduced legislation to facilitate the increased usage of the internet as a medium for business whilst insuring security.

---

* LLB (*Jor*), LLM (*Sud*), MIntTCL (*Macq*) PhD Candidate in Telecommunication Law, Department of Business Law, Faculty of Business and Economics, Macquarie University, Sydney, Australia.

** PhD Candidate, School of Information Systems, Faculty of Business, University of Southern Queensland (*USQ*), M.Sc in MIS University of Wollongong (*UOW*), MSc in Applied Finance, University of Western Sydney (*UWS*), Australia.

This study aims to examine the effectiveness of electronic signatures in facilitating the adoption and implementation of means of electronic commerce. This study also explores the legislative approaches that have been adopted in regulating electronic signatures around the world as well as the international legal framework.

II BACKGROUND TO ELECTRONIC SIGNATURES (ES)

There is no fixed legal definition of a traditional signature, many cases over the years, and many judges have defined signatures in different ways. Some of the reoccurring elements include: writing drawing or affixing[1], by one's own hand, one's own name or any mark which identifies it as the act of the party.[2] Rubber stamps with the name of a person or company also carry legal force to fulfil the requirements of a signature.[3] The courts have also recognized documents verified by a facsimile signature.[4] There, remain, however, some evidential problems caused by the acceptance of a facsimile signature as to the providing of assent essentially due to the fact that the placing of the signature was not witnessed by the recipient.[5] It is observed that the object of requiring a document to be signed by a person is to authenticate the verity of the document.

An electronic signature can be defined as 'any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with an intent to authenticate a writing'[6] or as any method which applies a signature to an electronic message.[7] On the international scene, the *United Nation (UNCITRAL) Model Law on Electronic Signature 2001* has defined electronic signature generically as

> Data in an electronic form in, affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data massage and indicate the signatory's approval of information contained in the data massage.[8]

---

1 *Electronic Rentals Pty Ltd v Anderson* (1971) 124 CLR 27 at 42.

2 *Morton v Copeland* (1855) 16 CB 517 at 535

3 *Goodman v Eban* (J) (1954) ALL ER 763 at 766

4 Mallesons Stephen Jaques, *The Pen-Op Signature : An Australia Legal Perspective* (2002) <http://www.ecomaus.com/legal%20documents/Australian%20Opinion.pdf > at 10 August 2007

5 Ibid.

6 Stephen E. Blythe, 'Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-commerce with Enhanced Security' (2005) XI (2) *Richmond Journal of Law and Technology* 1-20.

7 Alan Tyree et al, 'Banking Law and Banking Practice' (2006) 17 *Journal of Banking and Financial Law Practice,* 47-50.

8 *UNCITRAL The Model Law of Electronic Signature* (2001) <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html> at 10 October 2007.

Most European countries have transposed this definition into their national legislation. Alternatively some countries have narrowed the definition by specifying the particular purpose of authentication or the scope of definition down to the use of signature by a person.[9]

In Australia the definition of electronic signature is also based on the *UNCITRAL Model law*. Section 10 (1) (A) of the *Electronic Transaction Act 1999* (Cth) provides that the signature method adopted in an electronic transaction must identify the person and indicate their approval of the information. At the same time, the Australian Electronic Commerce Expert Group (AECEG) has defined an electronic signature as 'any symbol or method executed or adopted by a party with the present intention to be bound or to authenticate a record, accomplished by electronic means'.[10] This definition includes typing the name at the end of an electronic message; a digital fingerprint; or an algorithm or other mathematical sequence with unique identifiers.

A *How Electronic Signatures are Used*

To sign an electronic document by electronic means is the primary function of electronic signatures. These signatures are often made by converting handwritten signatures by scanning its image to a word-processed document or the more technologically advanced method of using cryptography (the method of cryptography is explained below).[11] Electronic signatures that rely on public key cryptography are called 'digital signatures'. These signatures are technology specific types of electronic signature.[12] Digital signatures use private and public key cryptographic technology as well as digital certificates that are usually issued by a reputable third party certification authority.

B *Comparison with Traditional Handwritten Signatures*

The handwritten signature as a legal device is something we owe to Roman law (as well as many other western legal tools). The subscription of

---

9 Jos Damortier et al, *The Legal and Market Aspects of Electronic Signatures* (2005) < http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf > at 11 September 2007.

10 Report of Expert Group to the Attorney General of Australia, *Electronic Commerce: Building the Legal Framework* (1998) <http://www.ag.gov.au/www/agd/agd.nsf/Page/e-commerce_Electroniccommerceexpertgroupsreport> at 2 August 2007.

11 American Bar Association, *Digital Signature Guidelines Tutorial*, <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html> at 5 August 2007.

12 *Towards A European Framework for Digital Signature and Encryption* <www.hermetic.ch/crypto/digsin.doc> at 5 August 2007.

signature at the end of a document was first used for authenticating wills as far back as 349 AD. From that time, the signing of any document by writing one's own name in order to authenticate it has became so popular that the system has stayed essentially unchanged for over 1,400 years.[13]

The trust for handwritten signatures in commerce is based on the use of secure paper (perhaps watermarked), handwriting styles, stamps, envelopes and even the personal contact between author and document.[14] The pith of handwritten signatures is a personally created symbol created with intent. According to the US commercial code 'any symbol made with intent to authenticate 'qualifies as a signature.[15] All signatures, whether handwritten or electronic, should embody three security measures. These are authentication, integrity and non-repudiation.

In terms of authentication, the purpose of this measure is ensuring the identity of the signature provider. The identity can be verified through means such as face to face meeting, telephone conversation, visits to the offices of other party to exchange of business card.[16] In relation to traditional banking services, when any person withdrew money from his or her account the bank clerk compared the signature on the form with the signature on banks files. This is a prime example of how handwritten signatures are used to verify that the person really was the owner of the bank account.[17] Other verification methods adopted to utilise the authenticity of documents signed by handwritten signatures is during a court proceeding witness may be called to verify the signature, or a person with knowledge of the person's signature or a handwriting specialist. Hence, when the handwritten signature is affixed to a document the signer cannot repudiate the signature.[18] In this respect electronic signatures are identical to handwritten signatures or at least serve the same function.[19] The second measure of 'integrity' means that a document which is signed by hand still does not provide any guarantee. In

---

13 David Fillingham, *A Comparison of Digital and Handwriting Signature* (1997) <http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/fillingham-sig.html> at 7 August 2007.

14 Yee Fen Lim, 'Digital Signature, Certification Authorities and the Law' (2002) 9 (3) *E-law Murdoch University Electronic Journal of Law*. < http://www.murdoch.edu.au/elaw/issues/v9n3/lim93nf.html > at 7 August 2007.

15 Ibid.

16 Ibid

17 Fillingham, above n 13.

18 Fen Lim, above n 14.

19 Stephen Mason, 'Electronic Signature –Evidence: The Evidential Issues Relating To Electronic signature – part 1' (2002) 18(3) *Computer Law and Security Report* 175-80.

case of handwritten signatures which are made on paper the integrity of the document signed can always be verified. Alterations made to the content of the document become impossible to incorporate without confirmation of the signatory. The discovery of changes made to content of a digital document is only possible when electronic signatures are used.[20] In addition, both handwritten and electronic signatures are at risk of forgery. Hence, digital signatures could be stored on a smart card which may be stolen and used if the password is carelessly made available. Handwritten signatures could not be copied in this way and any copy may be detected by an expert.[21]

III REGULATING ELECTRONIC SIGNATURES

As stated above, the electronic signature laws are formulated very differently in different jurisdictions. Three important factors were identified, the nature and reliability of electronic signatures, the liability of parties involved in electronic transactions and the cross-border recognition of electronic certificates and electronic signatures. This research paper will examine these aspects and both the national and the international responses to their resolution.

A *The Australian Response to Electronic Signatures*

In Australia the *Electronic Transaction Act 1999* (Cth) is based on the recommendations of the Australian Electronic Commerce Expert Group (AECEG). In its final report submitted to the Commonwealth Attorney General on March 1998 the AECEG recommended that the Commonwealth enacts legislation based on the United Nation Commission on Trade Law (UNCITRAL) Model Law on electronic commerce.[22] Legislation was thus enacted across Australia. The various Acts at Commonwealth and State level are based on two principles: 'function equivalence' which means that transactions conducted using paper documents and transaction conducted using electronic communication should be treated equally by the law; and

---

20 Arturo Ribagorda-Garacho, 'Electronic Signature at the Heart of Information Security Development: An Overview' (2004) V (3) *The European Journal for the Informatics Professional* 6-10. < http://www.upgrade-cepis.org/issues/2004/3/up5-3Ribagorda.pdf >.

21 Ibid

22 Aashish Srivastava, 'Electronic Signatures: Authentication Technologies from a Legal Perspective by H.M.Schellekens' (2006) 46 (2) *Jurimetrics: The Journal of Law, Science and Technology* 233-235.

'technology neutrality' which means that the law should not discriminate between different forms of technology.[23]

According to the concept of functional equivalence the Commonwealth Act provides that for the purpose of Commonwealth law, a transaction will not be invalid because it took place by means of one or more forms of electronic communication.[24] Under Commonwealth law there are requirements that can now be met to categorise the transaction as taking place in electronic form. These requirements are:

- The giving of information in writing[25];
- Providing a signature[26];
- Producing a document [27];
- Recording information and retaining a document[28].

The legislation does not however specify any particular technology reflecting the concept of technological neutrality which must be used for electronic signatures. Given the pace of technological development and change in this area, it was considered to be more appropriate for the market to determine issues such as the level of security and the level of reliability required for an electronic signature. Moreover, the *UNCITRAL Model Law* states that an electronic signature is considered to be reliable for the purpose of satisfying the requirement refereed in if:

(a) The signature creation data are, within the context in which they are used , linked to the signatory and to no other person;
(b) The signature creation data were , at the time of signing , under the control of the signatory and of no other person;
(c) Any alteration to the electronic signature , made after the time of signing , is detectable , and
(d) Where a purpose of legal requirement for a signature is to provide assurance as to the integrity of the information to which is relate, any

---

23 Sharon Christensen, 'The Statute of Frauds in Digital Age-Maintaining the Integrity of Signatures' (2003) 10 (4) *E-Law Murdoch University Electronic Journal of Law*. <http://www.murdoch.edu.au/elaw/issues/v10n4/christensen104.html> at 7 August 2007.

24 *Electronic Transaction Act* 1999 (Cth) s8

25 *Electronic Transaction Act* 1999 (Cth) s9

26 *Electronic Transaction Act* 1999 (Cth) s10

27 *Electronic Transaction Act* 1999 (Cth) s11

28 *Electronic Transaction Act* 1999 (Cth) s12

alteration made to that information after the time of the signing is detectable.[29]

B *International Responses to Electronic Signature*

1 *UNCITRAL*

On July 2001 the General Assembly of the United Nations adopted the UNCITRAL Model Law on Electronic Signature which was based on the Model Law proposed in 1996 for standardizing legislation on electronic commerce internationally. One of its aims was to introduce uniform legislation on electronic signatures in an endeavour to increase the level of harmonization of national legislation regulating the legal relationship arising from and develop in the internet.[30] The *UNICTRAL Model Law* introduces a new approach to the acknowledgment of the legal effectiveness of electronic signature technological neutrality. The *Model Law* provides for the adoption of a so called functional equivalent approach. Making electronic signatures the functional equivalent of had written signatures. Article 3 focuses on the functional equivalence of electronic signatures and states

> Where the law requires as a signature of a person, that requirement is met in relation to data message if an electronic signature is used to that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all circumstance, including any relevant agreement.

In article 3 of the *Model Law* the principle of technological neutrality for the different electronic methods is established and it also states that no provisions of the Model Law should be interpreted in such a way as to limit or deprive the law of its effectiveness any with respect to particular electronic techniques.

2 *European Union Directive*

In December, 1999 a European Parliament and Council directive established a legal framework for electronic signatures given the obvious potential of

---

29 Article 6 (3).

30 Nadina Foggetti, 'Electronic Signature: An Analysis of the Main European and International Legal Regulations' (2004) V (3) *the European Journal for the Informatics Professional* 39-46. < http://www.upgrade-cepis.org/issues/2004/3/up5-3Foggetti.pdf >.

electronic commerce. [31] The principles which were confirmed by the community directive were based on technological neutrality which is established by international legislation. Article 2 defines an electronic signature as follows:

- 'Simple electronic signature' means data in electronic form which is attached to or logically associated with the electronic data and which serves as a method of authentication.

- 'Advanced electronic signature' means an electronic signature which meets the following requirements:

  (a) It is uniquely linked to the signatory;
  (b) It is capable of identifying the signatory;
  (c) It is created using mean that the signatory can maintain under his sole control , and
  (d) It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Furthermore, a 'certificate advanced electronic signature' is where the identity of the signatory is confirmed by a certificate issued by an appropriate third party complying with other provisions of the directive (a qualified certificate) and the certificate is created by means of secure signature creation device. Also article 5 of the directive sets out the situations in which electronic signatures are to be valid, enforceable and legally effective. Member states had until July 2001 to enact conforming national legislation as of January 2001, five had enacted legislation (Australia, Denmark, Italy, Portugal and Spain) and six had proposed legislation (Denmark, Germany, Netherlands, Norway, Sweden, and United Kingdom). Some progress has since been made but not all nations have adopted the exact provisions of the directive to date.

3 *United States of America*

There are a number of states that have enacted their own legislation on electronic commerce and electronic signatures. These states have taken

---

[31] Report from the Commission of the European Parliament and Council, 'Report on the operation of Directive 1999/93/EC on a Community framework for Electronic Signatures' (2006) *Lex Europa* <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0120:FIN:EN:PDF> at 15 September 2007.

different approaches which have resulted in variations in the regulations between states.[32] For example, Utah, New Mexico, Mississippi, Missouri and Minnesota, have developed electronic signature agreements based on Public Key Infrastructure (PKI) technology and adopted a technology specific approach. California, Alabama, Arizona and other states have followed a totally different approach which is a technology neutral approach which covers multiple forms of electronic signatures giving them the same legal effect as handwritten signatures provided that electronic signatures meet certain requirements.[33] The *Uniform Electronic Transaction Act* (UETA) is one of the several US laws drafted and recommended by the National Conference of Commissioners on Uniform State Laws (NCCUSL) and defines an electronic signature as a symbol with the intent to sign the record.[34] This Act follows the principle of technology neutrality. No specific technology is required to be used in order to create a valid electronic signature. Nevertheless, both UETA and the *UNICTRAL Model Law* share the same purpose, which id to facilitate the use of and establish a uniform legal framework for electronic records and electronic signatures[35]

At the federal level of US regulation, there is the Electronic Records and Signatures in Commerce Act 2000 (or *Electronic Signatures Act*). Section 106 (5) of *Electronic Signature Act* defines an electronic signature as including electronic sounds, symbols or processes. Thus, assuming that the requisite intent is present, the following would succeed as electronic signatures:

- A manual signature transmitted by facsimile;
- Type name;
- Digested picture or image of manual signature;
- Biometrics;
- Digital signature;
- Clicking on a button labelled 'I agree' or 'purchase now';
- Voice on an answering machine and

---

32 Anda Lincoln, 'Electronic Signature Law and the need for Uniformity in Global Market' (2004) 8 *The Journal of Small and Emerging Business law* 67-86, 71.

33 Allison Freedman, 'The Electronic Transactions Act: Pre-empting State Law by Legislation Contradictory Technology Standard' (2001) *Utah Law Review* 807-842, 810.

34 *Uniform Electronic Transaction Act 1999* (US) s3 (7).

35 John Stolz and John Cromie, 'Electronic Signatures in Global and National Commerce Act' (2001) *American Bar Association* <http://www.cfg-lawfirm.com/article/oneleclick.html> at 10 October 2007.

- Including your name as part of an electronic mail communication or including firm name on facsimile.[36]

The only condition for any electronic sound, symbol or process to be qualified as signature is that it must reflect the intention to sign the electronic record.[37]

A signature may not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form.[38] The *Electronic Signature Act* states that a contract in relation to a transaction may not be denied legal effect, validity or enforceability on the sole ground that an electronic signature was used in the contract. These provisions are aimed at eliminating the uncertainty that businesses now face with respect the legal validity of their online business contracts.[39] However, the parties may decide by themselves if they want to use or accept electronic signature. On other hand, the Electronic Signature Act is silent about the certificate authorities who provide the third party certification services or the liability of the signatory or recipient. However, section 101(C) (1) (a) includes some consumer protection provisions. In the case that there is a requirement for the contract to be in writing in a consumer transaction this requires prior consent for the use of electronic means. If there happens to be any change to this requirement after consent, the consumer has the right to withdraw without any cost or liability.

The *Electronic Signature Act* applies to the use of electronic signatures in interstate or foreign commerce. The Act supports the use and acceptance of electronic signatures on the international level.[40] although, as Wang states, 'an electronic signature dose not establish detailed provision in relation to the recognition of certification services providers established in forging Jurisdictions'.[41]

---

36 David E Ewan, John A. Richards and Margo H K Tank, 'It's the Message, Not the Medium! Electronic Record and Electronic Signature Rules Preserve Existing Focus of the Law on Content, Not Medium of Recorded Land Title Instruments' (2006) 60 (4) *Businesses Lawyer* 1487-150.

37 Jonathan Stern, 'The Electronic Signature in Global and National Commerce Act' (2001) 16 *Berkeley Technology Law Journal* 391-414; See also *Electronic Signatures in Global and National Commerce Act* 2000 (US) s106 (5).

38 *Electronic Signatures in Global and National Commerce Act* 2000 (US) s101 (a) (1).

39 *Electronic Signatures in Global and National Commerce Act* 2000 (US) s101 (a) (2).

40 *Electronic Signatures in Global and National Commerce Act 2000* (US) s301 (a) (1).

41 Minyan Wang, 'Do the Regulations on Electronic Signatures Facilitate International Electronic Commerce? A Critical Review' (2007) 23 (1) *Computer Law and Security Report* 32-41.

4 *China*

In China, the first relevant regulation on e-commerce is the contract law which was issued in 1999. Article 11 provides that

> A written form means a memorandum of contract latter or data message (including telegram, telex, facsimtract, electronic data exchange and electronic mail), etc. which is capable of presenting its contents in a tangible form.[42]

However, it only recognizes a data message as a form of writing in law and says nothing of sole electronic signatures. This approach has been criticized as a simple equivalent approach because it keeps silent as to how an electronic contract performs the function of a paper document.[43] The contract law of 1999 did not consider the validity and enforceability of electronic signatures.[44]

In 2004 the Chinese *Electronic Signature Law* was enacted and promulgated and become effective in April 2005. The *Electronic Signature Law* explained the reasons for the enactment the law: (1) to grant electronic signatures the same legal status as the handwriting or sealed signature; (2) to regulate the procedure undertaken when using e-signature; and (3) to delineate the rights and responsibilities of the parties, the subscriber, the Certification Authority and other third parties. The law offers greater reliability for the use of electronic signatures and grants electronic signatures the same status as handwritten signatures, or signing a seal.[45] Art 13 of the *Electronic Signature Law* stipulates the following requirements: An electronic signature is deemed to be reliable electronic signature if the following requirements are met:

1. At the time the electronic signature creation data is used for an electronic signature, it is proprietary to the electronic signatory;

---

42 *Contract Law of the People's Republic of China* 1999, art 11.

43 Fuping Gao, 'The E-Commerce Legal Environment in China: Status Quo and Issues' (2004) 18 (1) *Temple International and Comparative Law Journal* 51-76.

44 Stephen Blythe, 'China's new Electronic Signature Law and Certification Authority Regulations: a Catalyst for Dramatic Future Growth of E-Commerce' (2007) 7 *Chicago – Kent Journal of Intellectual Property* 1-32. < http://jip.kentlaw.edu/art/volume%207/7%20chi-kent%20j%20intell%20prop%201.pdf > at 3 January 2008.

45 *Electronic Signature Law of the People's Republic of China* 2004, art 14.

2. At the time of signing , the electronic signature creation data is controlled solely by the electronic signatory;
3. Any change to the electronic signature after signing is noticeable; and
4. Any change to the content and form of the data message after signing is noticeable

These requirements are similar to the requirement for advanced electronic signature in German law. The *Electronic Signature Law* gives parties the ability to choose electronic signatures that meet the agreed reliability requirements of their particular transaction.[46] Moreover, some local authorities in China have issued some rules to govern electronic signatures especially in relation to electronic certification services. The first government rules to enact rules dealing with digital signatures were the *Hanian Administrative Measures on Digital Certification* in 2001. Shanghai also issued the *Shanghai Administrative Measure on Digital Certificates*. It was the first legislation in China to require the using of PKI technology and establish a governmental certificate authority. In 2002 Guaudong province passed the *Electronic Transaction Regulations*, which become the first laws to provide legal authority in court and cover electronic signature issues and certificate authorities.[47]

Art 26 of the *Electronic Signature Law* aims to facilitate cross-border transactions that are subject to verification by the MII (Ministry of Information Industry) on the basis of the principle of reciprocity of electronic signature certificates issued by electronic service providers outside China. These certificates shall have the same legal effect as electronic signature certificates issued by certification authorities established in accordance with Chinese law.[48]

IV CONCLUSION

This research refers to a number of model laws, directives and legislative instruments which support the implementation of a legal framework which validates the use of electronic signatures for commercial transactions. The Australian, U.S and Chinese approaches are based on the *UNCITRAL Model Law* and have adopted a function equivalence and technology neutral approach in order to achieve greater strictness and uniformity in their electronic signature laws.

---

46 *Electronic Signature Law of the People's Republic of China* 2004, art 13.
47 Blythe, above n 43.
48 *Electronic Signature Law of the Peoples Republic of China* 2004, art 26.

The European Union took a two tier approach and has provided a model worthy of emulation by other countries. Germany, for example, has based its approach on these EU directives but such directives lack some of the features of other systems. The US and China, by contrast, do not require the use of specific technology leaving them free to choose another form of electronic signature and avoid altogether the rather stringent regulatory rules that govern certification authorities. In this respect, the Australian government has developed a 'Gatekeeper' digital certificate approach aiming at higher security levels and authenticity requirements.

Electronic signatures must serve the same function as handwritten signatures. In any case, there is more than one type of electronic signature and more than one type of legal system seeking to regulate electronic signatures around the world. This technology provides new challenges. As these new challenges are met, jurisdictional harmony must be balanced against security and authenticity in the field of commercial transactions.