Electronic Signatures in Practice

By Stephen Mason, Barrister

Cite as: J. High Tech L. 148

Senior Research Fellow and Director of the Digital Evidence Research Programmeat the British Institute of International and Comparative Law; General Editor, Digital Evidence Journal; Associate Senior Research Fellow, Institute of Advanced Legal Studies

This article briefly outlines the case law in relation to manuscript signatures in England and Wales, putting the concept of manuscript signatures into historical perspective from the point of view of the common law. A short outline of the international framework for electronic signatures will follow, and consideration will be given to the three main concepts adopted by politicians in the form of legislation from across the world. The forms of electronic will be set out, and a number of practical and evidential issues will be taken into account. Relevant case law is considered throughout the article.

 ISSN 1536-7983

Introduction

Before the use of electronic signatures, successive judges in England and Wales, as well as other common law countries, took the view that the form a manuscript signature takes is not relevant, providing the function the signature performs is clear from the evidence. This pragmatic view of the imperfections of human behaviour has enabled judges to widen the concept of a signature, as set out briefly in the discussion below.

Manuscript signatures in England and Wales

The mark of a cross is an accepted form of signature, as demonstrated by the case of *Harrison v Harrison*.[1] In addition, the use of a pseudonym has been held acceptable,[2] as has the use of initials, since the 1808 case of *Phillimore v Barry*.[3] The decision by Matheson J in *Re Schultz*[4] serves to reinforce the point that the difference in time or jurisdiction does not alter the underlying rationale of this line of thinking. Similar examples demonstrate the inherent flexibility of this approach, in that a surname has been held sufficient to authenticate a document,[5] as has a trade name,[6] a partial signature,[7] words other than a name,[8] an identifying phrase[9] and an abbreviation of a name.[10]

Impression of a mark

Seals have a long history, and name seals remain in common use in Japan. There are two forms in Japan: the Jitsuin (official or legal seal) and mitomein (personal seals). Any type of name seal can serve as a mitomein, but a Jitsuin must be registered. Jitsuins are used instead of manuscript signatures to execute important documents. The first recorded case relating to the use of a seal in England and Wales dates from 1681.[11] In this instance, the devisor added his seal to his will in front of the three witnesses, but did not add his manuscript signature. In a somewhat ambiguous decision, it was held, with Levinz, J. dissenting, that the act of using the seal was a sufficient mark. This

1. Harrison v Harrison (1803) 8 Ves Jun 185; 32 ER 324.
2. *In re* Reddings Goods (1850) 14 Jur 1052; 2 Rob Ecc 338; 163 ER 1338.
3. Phillimore v Barry 1 Camp 512; 170 ER 1040.
4. *In re* Schultz, (1984) 8 DLR (4th) 147.
5. *Lobb and Knight v Stanley* (1844) 5 QB 574; 114 ER 1366.
6. *Cohen v Roche* [1927] 1 KB 169.
7. *Chalcraft, Re, Chalcraft v Giles* [1948] P 222.
8. *Cook's Estate, Re, Murison v Cook* [1960] 1 All ER 689.
9. *Selby v Selby* (1817) 3 Mer 2; 36 ER 1.
10. *Bartletts de Reya v Bryne* (1983) The Times 14 January; (1983) 127 SJ 69.
11. *Lemayne v Stanley* (1681) 3 Lev 2; 83 ER 545.

decision was not acceptable to some judges, and by 1754,[12] it was established that the use of a seal was not capable of authenticating a document. However, a number of nineteenth century cases subsequently accepted the possibility that a seal was capable of acting as a means of authentication.[13] Further examples of impressions that have been held acceptable as authenticating a document include the use of a printed name[14] and a stamp.[15]

Mechanical marks by human action

Modern technology has never been an obstacle to judges in applying underlying legal principles, as demonstrated by the use of a telex to enter a contract, which was the subject of discussion in the case of *Clipper Maritime Ltd v Shirlstar Container Transport Ltd, The Anemone*,[16] and the transmission of a proxy form by way of a facsimile transmission, which was considered in 1995.[17]

Electronic signature legislation

Several international organizations produced guidelines in relation to the manifestation of electronic signatures at the turn of the centuries. These include two United Nations Commission on International Trade Law (UNCITRAL) Model Laws, on Electronic Commerce[18] and Electronic Signatures.[19] The International Chamber of Commerce (ICC) produced a further document entitled 'General Usage for International Digitally Ensured Commerce' (GUIDEC).[20] The UNCITRAL model laws are designed to encourage harmonization of laws across member states, and the ICC document seeks to allocate risk and liability between parties that are in line with current

12. *Ellis v Smith* (1754) 1 Ves Jun 11; 1 Ves Jun Supp 1; 30 ER 205; 34 ER 666.

13. The last case was *Lemon's Good, Re* (1896) 30 Ir LTR 127.

14. *Saunderson v Jackson* (1800) 2 Bos & Pul 238; 126 ER 1257.

15. J *Jenkins v Gainsford and Thring* (1863) 3 Sw & Tr 93; 164 ER 1208; (1862 – 63) 11 WR 854 is the first of a number of cases ending in *Goodman v J Eban Limited* [1954] 1 QB 550; [1954] 1 All ER 763; [1954] 2 WLR 581, CA and *British Estate Investment Society Ltd v Jackson (H M Inspector of Taxes)* (1954 – 1958) 37 Tax Cas 79; [1956] TR 397; 35 ATC 413; 50 R & IT 33.

16. *Clipper Maritime Ltd v Shirlstar Container Transport Ltd, The Anemone* [1987] 1 Lloyd's Rep 546.

17. *Re a debtor (No 2021 of 1995), Ex p, Inland Revenue Commissioners v The debtor; Re a debtor (No 2022 of 1995), Ex p, Inland Revenue Commissioners v The debtor* [1996] 2 All ER 345, Ch D, and *Standard Bank London Limited v Bank of Tokyo Limited* [1995] CLC 496; [1996] 1 CTLR T-17.

18. UNCITRAL Model Law on Electronic Commerce (1996), *available in electronic format at* http://www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/. Includes the addition of an article 5 bis as adopted in 1998 and Guide to Enactment.

19. UNCITRAL Model Law on Electronic Signatures 2001, *available in electronic format at* http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf.

20. General Usage for International Digitally Ensured Commerce, *available in electronic format at* http://www.iccwbo.org/home/guidec/guidec_one/guidec.asp; http://www.iccwbo.org/home/news_archives/2001/guidec_two.asp.

business practices.

Approaches to legislation
Functional equivalent concept

In many civil law jurisdictions, the digital signature is considered to have a greater legal effect than other forms of electronic signature. For instance, many of the states in Latin America have developed laws based on the UNCITRAL Model Law on Electronic Signatures and the European Union (EU) Directive. Although there is an emphasis on the digital signature as the functional equivalent of a manuscript signature, the legislation also permits the use of other forms of electronic signature, which suggests a two-tier approach as discussed below. One example is the Ley De Firma Digital[21] Nº 25.506 passed by Argentina in 2001, which provides for the functional equivalent of a manuscript signature in article 3, in that a digital signature is considered to be the equivalent of a manuscript signature:

"ARTICULO 3º — Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia."[22]

"ARTICLE 3.- On the requirement of signature. When the law requires a handwritten signature, this requirement is also met by a digital signature. This principle is applicable to those cases in which the law establishes the obligation of signing or prescribes consequences for the absence of a signature."

Where a digital signature is used, the legislation requires it to be verified by a third party by way of the Application Authority, and the verification serves not only to identify the signing party, but is required to detect any alteration to the document after it has been signed. In addition, there is a requirement that the digital signature be controlled by the signing party and be under their absolute control, as provided for in article 2:

"ARTICULO 2º — Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con

21. Law No. 25.506, Dec. 11, 2001, B.O. *available in electronic format at* http://www.certificadodigital.com.ar/ley25_506.htm.

22. *Id.* at articulo 3º.

estándares tecnológicos internacionales vigentes."[23]

"ARTICLE 2.- Digital Signature. A digital signature is the result of applying a mathematical procedure to a digital document, that requires information controlled exclusively by the signing party and which is under his absolute control. The digital signature must be verifiable by third parties, such that this verification will simultaneously permit the identification of the signing party and detect any alteration of the digital document after it has been signed.

The signature and verification procedures to be used for this purpose shall be those established by the Application Authority in accordance with current international technological standards."

Other forms of electronic signature are not recognized as the functional equivalent of a manuscript signature unless the parties mutually recognize the form of signature that is used. If a party relies on any other form of electronic signature, it is for them to prove its validity, as provided for in article 5:

"ARTICULO 5º — Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez."

"ARTICLE 5.- Electronic signature. An electronic signature is a set of integrated electronic data, linked or associated logically to other electronic data, used by the signing party as his means of identification, which lacks any of the necessary requirements to be considered a digital signature. If an electronic signature is not recognized, it is up to the party that invokes it to prove its validity."

The minimalist approach

Australia,[24] Canada,[25] Guernsey,[26] and the United States of America[27] have adopted this approach. To a certain extent, this is the approach taken in the United Kingdom with the Electronic Communications Act 2000. In common law countries, the emphasis on form, rather than function, means the weight of the evidence is far more important in determining a person's intention, rather than the form that their signature took.[28] The Australian government deals with

23. *Id.* at articulo 2º.

24. Electronic Transactions Act, 1999, c. 2 (Austl.).

25. The Uniform Law Conference of Canada: The Uniform Electronic Commerce Act, *available at* http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u1

26. The Electronic Transactions Law, 2000 (Guernsey), *available in electronic format at* http://www.asianlaws.org/cyberlaw/library/legislations/ecom/guernsey.pdf.

27. Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7006 (2000).

28. For a discussion of the case law in the United Kingdom since 1681, see STEPHEN MASON, ELECTRONIC SIGNATURES IN LAW, ch. 2 (LexisNexis Butterworths, 2003) , LORNA BRAZELL, ELECTRONIC

the legal effect of electronic signatures, which are reflected in the provisions of §10 of the Electronic Transactions Act[29]:

"10 Signature

Requirement for signature

If, under a law of the Commonwealth, the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if:

(a) in all cases—a method is used to identify the person and to indicate the person's approval of the information communicated; and

(b) in all cases—having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated; and

(c) if the signature is required to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that the method used as mentioned in paragraph (a) be in accordance with particular information technology requirements—the entity's requirement has been met; and

(d) if the signature is required to be given to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity—the person to whom the signature is required to be given consents to that requirement being met by way of the use of the method mentioned in paragraph (a)."

The focus is on the method used to communicate intention and to ensure the method chosen is appropriate for the purposes of the information. As a result, an "I accept" icon can be effective when used to indicate the agreement for the purchase of goods or services from a trader operating a web site. There is no need for the complexity associated with the use of a digital signature to prove intent. The important issue is whether the intent is manifest and the method is appropriate to the particular transaction.

Of interest, the Canadians have replaced the concept of an original document with proof of the reliability of a system, instead of the reliability of an individual record. The application of standards demonstrate the reliability of a system, although the Uniform Act also permits, in §10(2) a standard of reliability to be imposed where it is considered necessary by the relevant authority:

"Signatures

10. (1) A requirement under [enacting jurisdiction] law for the signature of a person is satisfied by an electronic signature.

(2) For the purposes of subsection (1), the [authority responsible for the requirement] may make a regulation that,

SIGNATURES LAW AND REGULATION, ¶¶ 2-016 – 2-037 (Sweet & Maxwell, 2004).

29. Electronic Transactions Act, *supra* note 24 at §10.

(a) the electronic signature shall be reliable for the purpose of identifying the person, in the light of all the circumstances, including any relevant agreement and the time the electronic signature was made; and

(b) the association of the electronic signature with the relevant electronic document shall be reliable for the purpose for which the electronic document was made, in the light of all the circumstances, including any relevant agreement and the time the electronic signature was made.

(3) For the purposes of subsection (1), where the signature or signed document is to be provided to the Government, the requirement is satisfied only if

(a) the Government or the part of Government to which the information is to be provided has consented to accept electronic signatures; and

(b) the electronic document meets the information technology standards and requirements as to method and as to reliability of the signature, if any, established by the Government or part of Government, as the case may be."

The aim is to link a person to a document, and §10 seeks to ensure an electronic signature functions as a signature in law. The person creating or adopting the document in electronic format must have the requisite intent and their intent must be associated to the document in some way.

The two-tier approach

The United Nations adopted the two-tier approach in the Model Law on Electronic Commerce. Article 7 of the UNCITRAL Model Law on Electronic Commerce, considers the form of an electronic signature and whether it is appropriate in the circumstances[30]:

"Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature."

The Model Law on Electronic Signatures takes one step further by incorporating the provisions of article 7 of the Model Law on Electronic Commerce, and adding a provision relating to the reliability of a signature[31]:

30. UNCITRAL Model Law on Electronic Commerce, *supra* note 18 at Art. 7.

31. UNCITRAL Model Law on Electronic Signatures, *supra* note 19 at Art. 6

"Article 6 Compliance with a requirement for a signature

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

2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 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 the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

4. Paragraph 3 does not limit the ability of any person:

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or

(b) To adduce evidence of the non-reliability of an electronic signature.

The legal effect that follows the use of an electronic signature is left for the enacting state.

Singapore,[32] Bermuda[33] and the European Union[34] followed this model. For instance, the EU Electronic Signatures Directive distinguishes between an electronic signature and a qualified certificate. The directive defines an electronic signature as:

"'electronic signature' means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;"[35]

An electronic signature is admissible in evidence if it complies with the definition in article 2(1), although it only serves to authenticate data. In

32. Electronic Transactions Act 1998 (Sing.), *available in electronic format at* http://www.ida.gov.sg/idaweb/doc/download/I1934/Legal_Guide_1998.pdf .

33. Electronic Transaction Act 1999 (Berm.), *available in electronic format at* http://www.bakernet.com/ecommerce/bermuda-eta.doc.

34. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L13/12 19 January 2000).

35. (OJ L13/12 19 January 2000), Article 2(1).

contrast, a qualified certificate is capable of identifying a person or entity. To be admissible, an advanced electronic signature must have a qualified certificate and it is required to be created by a secure-signature-creation device. The necessary technical requirements are set out in Annex I, and a qualified certificate must be provided by a certification-service-provider who fulfils the stipulations set out in Annex II.

The Singapore legislation differentiates between electronic signatures and secure electronic signatures. The Act provides that an electronic signature can be proved in any manner, as provided for in §8[36]:

"8. Electronic signatures

(1) Where a rule of law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of such party."

The definition of a secure electronic signature (§17), in contrast, is very similar to the advanced electronic signature set out in article 2(2) of the EU Directive**.**

Bermuda consciously drew from the UNCITRAL Model Law on Electronic Commerce, the EU Directive and legislation from other jurisdictions, in particular that of Singapore. The Electronic Transaction Act 1999 provides for two types of signature, depending on the use to which they are put. Part II, §11 of the Bermudan Act, refers to the form an electronic signature should take that will meet the criteria where a signature is required by law when used to identify a person intending to sign or otherwise adopt the content of a document in electronic format. This provision permits the use of different types of electronic signature, other than a digital signature, as set out in section 11:

Signature

11(1)Where the signature of a person is required by law, that requirement is met by an electronic record if—

(a)a method is used to identify that person and to indicate that the person intended to sign or otherwise adopt the information in the electronic record; and

(b)that method is as reliable as is appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement.

However, where a signature is required by law, Part IV of the Act, in

36. Electronic Transaction Act 1998 (Sing.), *supra* note 32 at §8.

referring to electronic signatures, makes it clear that to satisfy the requirements of §11(1)(a) and (b), the electronic signature must be associated with an accredited certificate, making it a digital signature in all but name, as set out in section 19:

Electronic signature associated with an accredited certificate

19An electronic signature that is associated with an accredited certificate issued by an authorised certification service provider under section 20 is deemed to satisfy the requirements of subsection 11(1)(a) and (b).

As a result, Bermuda has taken the view that a digital signature must be used where the law requires a manuscript signature.

Forms of electronic signature

There are various types of signature, all of which can demonstrate the intent of the signing party to authenticate the document. The different types are:

When a person types their name on to a file in electronic format, such as a letter, e-mail or other form of document, the text added is a form of electronic signature. This was the subject of discussion in England and Wales in the case of *Hall v. Cognos Ltd.*.[37] In this case, the chairman of the Tribunal determined that a name typed into an e-mail was a form of signature. Although no relevant case law was mentioned in this instance, the decision was consistent with decisions made by judges in England and Wales since the seventeenth century, illustrating that the function of a signature overrides the form it takes. Case law applying electronic signature statutes in the United States of America indicates the acceptance of this form of electronic signature[38], as does a recent case in Singapore.[39]

The 'click wrap' method of indicating intent, namely clicking the "I accept" icon to confirm the intention to enter a contract when buying goods or services electronically.

A Personal Identification Number (PIN), used to obtain money from cash machines or to 'sign' a credit card with a PIN.

A biodynamic version of a manuscript signature; a special pen and pad measure and record the actions of the person as they sign. This creates a digital

37. *Hall v. Cognos Limited,* Hull Industrial Tribunal Case No 1803325/97.

38. *See* Shattuck v. Klotzbach, 14 Mass. L. Rptr. 360 (Mass. Super. Ct. 2001); *see also* Sea-Land Serv., Inc. v. Lozen Int'l, LLC., 285 F.3d 808 (9th Cir. 2002); *see also* Cloud Corp. v. Hasbro, Inc,. 314 F.3d 289 (7th Cir. 2002); *see also* Roger Edwards, LLC. v. Fiddes & Son Ltd., 245 F. Supp. 2d 251 (D. Me. 2003); *see also* On Line Power Tech., Inc. v. Squared D Company, 2004 WL 1171405 (S.D.N.Y.); *but see* Toghiyany v. Amerigas Propane, Inc., 309 F.3d 1088 (8th Cir. 2002).

39. SM Integrated Transware Pte Ltd. v. Schenker Singapore (Pte) Ltd., [2005] SGHC 58. For a case report on this case by Bryan Tan, *see* E-SIGNATURE LAW JOURNAL, vol. 2, no. 2 (2005), at 126 – 27.

version of the manuscript signature. The file can then be attached to electronic documents.

A scanned manuscript signature; a manuscript signature is scanned and transformed into digital format, which can then be attached to an electronic document.

The digital (or cryptographic) signature, which uses cryptography. The signing party uses a key pair (private and public key). The sender affixes the signature using their private key,and the recipient checks the signature with the public key.

The form of an electronic signature will have a bearing on its legal and evidential effect. However, it should also be observed that the elements that make up the definition of an electronic signature, and the presumptions that apply, will also affect its legal acceptance in a given jurisdiction. To sum up, there is no world-wide accepted definition of what constitutes an electronic signature. Furthermore,there is no agreement about the elements of an electronic signature, nor is there any agreement about the functional equivalence of an electronic signature. Finally, there is no clarity about the evidential presumptions relating to the use of electronic signatures.

The functions of a signature

Of interest is the way electronic documents are authenticated. The role of the notary public is less well known in common law countries, although it is interesting to note that the National Notary Association of the United States of America has appointed a Director of eNotarization. The approach taken by the State Bar of Notaries in Austria demonstrates that it is possible to provide for the authentication of documents electronically, given the legal framework established in Austria.[40] It will be interesting to observe whether greater use of such services will become ubiquitous. For instance, in common law countries, contracts tend to be exchanged between the parties. Each party will probably have an original copy of the document, if it is in writing, and both copies will be signed with a manuscript signature. Each copy will be both an original and a copy of the document. However, in many civil law jurisdictions, the public notary will retain the only original document, and the parties will be assured that the trusted third party will retain the original intact.

Invariably, the authentication of a document will depend on the function a signature performs. In summary, a signature can serve a number of functions, some of which are set out below, each of which can have varying degrees of importance:[41]

40. **Friedrich Schwank, *CyberDOC and e-Government: the electronic archive of Austrian notaries*, E-SIGNATURE LAW JOURNAL, vol. 1, no. 1 (2004), at 28 - 30.**

41. *See* Mason, *supra* note 28 at ¶¶ 2.110 – 2.117 (including a detailed discussion).

The primary evidential function, serving to provide admissible and reliable evidence that the signatory approves and adopts the contents of the document, and to demonstrate that is shall be binding upon the parties and shall have legal effect.

Secondary evidential functions, for instance where a signature is capable of authenticating the identity of the person signing the document.

Cautionary function, where the signature acts to reinforce the legal nature of the document.

A protective function, in that there is tangible the proof of the source and contents of the document.

Enforceability

Several factors will have a bearing on the enforceability of an electronic signature. They include the elements that define the signature, provisions relating to form and any presumptions that apply. Each will be treated briefly in turn.

Elements

The elements that make up the definition of an electronic signature can demonstrate difficulties for the international acceptance of a particular form of signature. For instance, the UNCITRAL Model Law on Electronic Commerce provides, in article 7(1)(a) provides for methods that are used to identify a person, and to indicate their approval of the information contained in the message. Whilst not precluding any other form of electronic signature, this definition presupposes that only a digital signature will suffice. This is reinforced by the provisions of article 7(1)(b), which discusses the issue of reliability and whether the form of signature is appropriate in the circumstances:

Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:(a) a method is used to identify that person and to indicate that person''s approval of the information contained in the data message; and

(b)_ that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

The problem is that reliability does not demonstrate a link between the owner of the signature and the act of affixing or linking the signature to the data message.

The UNCITRAL Model Law on Electronic Signatures also sets out a

definition in article 2(a)[42]:

"Electronic signature" means data in 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 message and to indicate the signatory's approval of the information contained in the data message;"

The aim, as set out in paragraphs 93 and 94 of the accompanying Guide to the Model Law, is to have two elements: for the electronic signature data to identify the signatory and to provide for the signatory's approval of the content of the message. Not all manuscript signatures operate to approve the content of a document – a witness signing a will is but one example.

The same comments can be made in relation to the EU Electronic Signature Directive, in that the electronic signature under the provisions of article 2(1) serves as a method of authentication. Unfortunately, this definition fails to link the need for the electronic signature to authenticate the data to which it is attached or logically associated. It is not clear whether the authentication relates to the origin of the data, or acts to verify the identity of a person or entity.

By contrast, the United States has approached the definition by taking a functionalist approach, as set out in §7006(5) of the Electronic Signatures in Global and National Commerce Act, states[43]:

"(5) ELECTRONIC SIGNATURE. - The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

The definition provides a number of elements, the most important of which is that the signature is "adopted by a person with the intent to sign the record."[44] This part of the definition permits any form of electronic signature to effect the function of demonstrating intent.

In summary, the elements of an electronic signature differ from jurisdiction to jurisdiction. Whether this will ever have an effect on trade is another matter. At present, there is little evidence that such differences have any bearing on international trade in practice. However, given the fact that the use of e-mail has become very common, it is highly probable that contracts are formed every day with the exchange of e-mail communications, both by individuals and business, and across international boundaries.[45] Where a challenge is made over the use of an electronic signature, care must be made to become more fully aware of the intricate details of the relevant statues relating to electronic signatures. An example is the Greek case of No 1327/2001 – Payment Order, before the Court of First Instance of Athens. In this case, a Czech agent

42. UNCITRAL Model Law on Electronic Signatures, *supra* note 19 at Art. 2(a).

43. Electronic Signatures in Global and National Commerce Act, *supra* note 27 at §7006(5).

44. *Id.*

45. *See, e.g.,* Roger Edwards, LLC. v. Fiddes & Son Ltd., 245 F. Supp. 2d. 251 (D. Me. 2003).

concluded a service agreement with Greek travel agency by way of an exchange of e-mail correspondence. A dispute occurred, and the judge upheld the complaint of the Czech agent by recognising the validity and the binding effect of the legal acts that were exchanged through the e-mail communications. The learned judge in the opinion of the author, correctly accepted the probative force of the e-mail exchange in this instance.[46]

Provisions relating to form

A document may only be acceptable for certain types of transaction if it conforms to a particular form. Examples include the formation of a will, the sale or lease of land, or the assignment of intellectual property rights. Whether a transaction complies with the necessary form will depend on the applicable law, or both the applicable law and any relevant rules of evidence. Rules of evidence may be express or implied, and such rules may serve to limit the ability to use the evidence of an electronic signature to demonstrate either the attrition of a message to its purported originator, or whether an electronic signature is an appropriate method to meet the formal legal requirements of a signature.

The interpretation of form varies between jurisdictions. The liberal approach is illustrated by an example from the United States of America in the case of a breach of contract. In *Cloud Corporation v. Hasbro, Inc.*,[47] the defendant denied placing orders. The parties communicated by way of e-mail, and the appeal court held that the sender's name in an e-mail satisfied the signature requirement of the statute of frauds. In the Columbian case of *Juan Carlos Samper Posada v. Jaime Tapias, Hector Cediel and others*,[48] the defendants sent unsolicited commercial e-mails to Mr Samper. Mr Samper took the time and trouble, by way of e-mail, to ask the defendants to refrain from sending him spam. Although the defendants repeatedly assured Mr Samper that they would take him off the e-mail list, he had to take legal action to enforce his rights not to be sent unsolicited commercial e-mail. Of interest was the assertion by the defendants that the court was not empowered to hear the matter, because both parties lived in Bogotá. However, the learned judge indicated it was rather ironic that defendants who used cyber space should argue over the venue for a court case. In addition, the defendants argued that the court proceedings were not valid because they did not include the use of

46. For a case note in English, see Georgia Skouma, *Case Note*, E-SIGNATURE LAW JOURNAL, vol. 1, no. 2 (2004), at 95 – 98.

47. Cloud Corp. v. Hasbro, Inc., 314 F.3d 289 (7th Cir., 2002).

48. Juan Carlos Samper Posada v. Jaime Tapias, Hector Cediel, Decisión 73-624-40-89-002-2003-053-00, July 21, 2003, Municipal Court of Rovira, Tolima, *available in electronic format at* http://www.alfa-redi.org/upload/revista/80403--0-7-diaz082003.pdf; *see also* Valeria Frigeri and Manuel F Quinche, Case Note, E-SIGNATURE LAW JOURNAL, vol. 2, no. 1 (2005), at 65 - 72.

digital signatures. In response, the judge took the opportunity of considering article 6 of the Ley Por No. 527 de agosto 18 de 1999 medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.Article 6 reads[49]:

"Artículo 6°. Escrito. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.

Article 6th. Written. Whenever any regulation requires the information to be in writing, such requirement will be satisfied by a data message; if the information such message contains is accessible for its later consultation.

The provisions in this article will apply both, if the requirement established in any regulation constitutes an obligation, and if the regulations anticipate consequences in case the information is not in writing."

The learned judge indicated that where regulations require the information to be sent in writing, an e-mail is sufficient, provided the parties are able to obtain access to the e-mail at a later date.

The French courts have taken a more restrictive approach, although it should be noted that the case mentioned below pre-dates the introduction of the French law on electronic signatures, and the decision may well be different now. In the case of *Société Chalets Boisson v. M. X*[50] the council of the Society Chalets Boisson entered an appeal before the Cour d'Appel of Besançon against a decision of a Conseil de prud'hommes (employment tribunal). The notice of appeal was sent to the office of the clerk of the court by e-mail, bearing an electronic signature. The defendant sought to have this appeal declared invalid, because the electronic signature was deemed not to identify the signatory. The Cour d'appel of Besançon accepted this argument and then declared this appeal inadmissible. The Cour de Cassation approved the Cour de Besançon decision. For an order to be valid, an appeal must be signed by its author and that an electronic signature, before the 13th March 2000 Act,[51] was not sufficient to identify the author. The comments by Philippe Bazin bear repeating:

".... judges at the time (and unfortunately still today) did not have any technical understanding about what these notions concretely represent. These

49. Ley Por No. 527, Artículo 6°, *availiable in electronic format at* http://www.sice.oas.org/e-comm/legislation/col2.asp

50. Cour de Cassation, Cass.2e civ. chambre civile 2, April 30, 2003, Case No 00-46467, *available in electronic format at* http:// www.juriscom.net/jpt/visu.php?ID=239; *see also* Philippe Bazin, Case Note E-SIGNATURE LAW JOURNAL, vol. 1, no. 2 (2004), at 93 – 94.

51. Law No. 2000-230 of March 13, 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative á la signature électronique.

that they know, they have practiced for a long time, and they have to do with paper, not the electronic environment.

In the April 30 2003 decision, the Court adopted a systematic position of mistrust with respect to the electronic signature. It confirms that – culturally – it is the paper, and only the paper, that constitutes the only solid legal guarantee."[52] In some jurisdictions, it may well be that this attitude might persist for some time.

Presumptions

Where an electronic signature is considered as a functional equivalent of a manuscript signature, some countries have included a number of presumptions in the legislation, such as article 3 of the Japanese Law Concerning Electronic Signatures and Certification Services (Law No.102 of 2000):

Article 3:

An electro-magnetic record which is made in order to express information (with the exception of one drawn by a public official in the exercise of his official functions) shall be presumed to be authentic if an electronic signature (limited to those that, if based on the proper control of the codes and objects necessary to perform the signature, only that person can substantially perform) is performed by the principal in relation to information recorded in the electro-magnetic record.

The recently enacted Electronic Signatures Law of People's Republic of China has a similar presumption, as set out in article 9, which is subject to a number of conditions: [53]

"Article 9: A data message is deemed to be sent by the originator if any of the following conditions has been met:

It was sent under the authorization of the originator;

It was sent automatically by the originator's information system;

The addressee verifies and ascertains the data message by a method ratified by the originator.

If the parties have agreed otherwise, such agreement prevails."

To a certain extent, the presumptions illustrated above demonstrate that the same presumptions apply in the digital world as they do in the real world in relation to manuscript signatures. The difference may be with respect to the costs of proof: evidence in digital format is more expensive in terms of the expertise required to analyse a computer or computer network. In this respect, lawyers, to fully advise their clients when dealing with international contracts,

52. *See* Bazin, *supra* note 50.

53. Passed by No. 11 meeting of No. 10 Standard Committee of the National People's Congress on 28 August 2004. For a translation into English by Minyan Wang and Minju Wang, *see* E-SIGNATURE LAW JOURNAL, vol. 2, no. 1 (2004), at 35 - 41.

must be aware of the differences between jurisdictions with respect to the legal presumptions that apply to difference forms of electronic signature.

Concluding remarks

As demonstrated in this article, it is necessary to be aware of the presumptions relating to the use of electronic signatures across jurisdictions. What might be acceptable in one jurisdiction will not necessarily be enforceable in another, unless due care has been taken to establish whether the format of a particular form of electronic signature is enforceable. It is too early to predict how electronic signatures in a formal context will develop, but the rush by legislators across the world to provide for the complexity of digital signatures as a functional equivalent of a manuscript signature was somewhat premature. Click wrap signatures did not require any form of legislation, yet this particular form of signature remains a form of electronic signature, despite the imposition of a highly technical response by way of legislation to what is a relatively simple legal issue. For lawyers, the central issue will be how to prove the nexus between the application of the signature, whatever form it takes, and the person whose signature it purports to be. Even where there is a presumption that the person used a digital signature whose signature it was issued to, there remains in the legislation the possibility of challenging such a presumption.

Stephen Mason is the author of *Electronic Signatures in Law* (LexisNexis Butterworths, 2003), *Networked communications and compliance with the law* (xpl publishing, 5th ed., 2005), the electronic and digital signatures editor and author of Chapter VI 'Electronic and Digital Signatures' for the practitioner loose-leaf textbook by M-T. Michéle Rennie *International Computer and Internet Contracts and Law* (Sweet & Maxwell), and the general editor of the *Digital Evidence Journal*.

s.mason@biicl.org

stephenmason@stephenmason.co.uk