DIGITAL SIGNATURE LAW OF THE UNITED NATIONS, EUROPEAN UNION, UNITED KINGDOM AND UNITED STATES: PROMOTION OF GROWTH IN E-COMMERCE WITH ENHANCED SECURITY

Stephen E. Blythe, Ph.D., J.D., LL.M.[*]

Cite as: Stephen E. Blythe, *Digital Signature Law of the United Nations, European Union, United Kingdom and United Stats: Promotion of Growth in E-Commerce with Enhanced Security*, 11 RICH. J.L. & TECH. 2 (2005), *at* http://law.richmond.edu/jolt/v11i2/article6.pdf.

[1] *Abstract:* Digital signatures enhance the ability of contracting parties to authenticate electronic communication. Sophisticated encryption and decryption technology is used to verify the identity of the other party to the electronic transaction. Digital signature law, necessary for adjudication of disputes between parties in e-commerce, is still in its infancy. This article covers basic digital signature law of the United Nations, the European Union, the United Kingdom, and the United States.

[2] The United Nations' Model Law of Electronic Commerce of 1996 ("MLEC") had many implications. The MLEC approved the utilization of electronic signatures, stated that electronic signatures would have the same legal impact as an ink signature, and remained technologically-neutral, *i.e.*, did not mandate the utilization of any specific type of technology.

[3] The admissibility of "advanced" electronic signatures in legal proceedings and seemed to favor the more sophisticated technologies such as public-key-infrastructure ("PKI"). Utilization of PKI would provide the ultimate in digital signature security.

[*] Stephen E. Blythe is Professor of Business at Warner Southern College in Florida. His mailing address is: 13895 Highway 27, Lake Wales, Florida 33859, and he can be reached by telephone at (863) 734-5132 (office), (863) 605-3085 (mobile), and (863) 638-3298 (home), and by facsimile at (863) 638-4907. His e-mail address is: itlawforever@netscape.net.

[4] The United Kingdom enacted the Electronic Communications Act in 2000. The Act recognized the validity of electronic signatures and affirmed their admissibility as evidence in court. Furthermore, the United Kingdom's Electronic Signatures Regulations went into force in 2002. The purpose of the regulations was to implement certain provisions of the European Union's E-Signatures Directive. However, the United Kingdom remained technologically-neutral.

[5] In the 1990s, most states in the United States adopted some form of the Uniform Electronic Transactions Act, which mandates broad recognition of electronic signatures. In order to achieve more uniformity in the laws of the states, the United States. federal government enacted "E-Sign" in 2000, which preempted all existing state law unless it was the original form of the Uniform Electronic Transactions Act. Unfortunately, United States jurisdictions now have a "patchwork quilt" of dissimilar law regarding digital signatures. The United States is technologically-neutral.

[6] The article concludes with recommendations for improvement of digital signature laws.

I. OBJECTIVES OF THE ARTICLE

[7] The objectives of this article are as follows: (1) to identify the several types of electronic signatures; (2) to explain PKI technology and how it makes digital signatures more effective than other types of electronic signatures; (3) to provide a concise summary of U.N., EU, U.K., and U.S. digital signature and e-commerce law; (4) to evaluate the law in terms of its facilitation of e-commerce, and to recommend changes in the law in order to encourage a greater use of e-commerce.

II. ELECTRONIC SIGNATURES

[8] Contract law worldwide has traditionally required the parties to affix their signatures to a document.[1] With the onset of the electronic age, the electronic signature made its appearance. An electronic signature has been 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,"[2] or as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."[3] An electronic signature may take a number of forms: a digital signature, a digitized fingerprint, a retinal scan, a pin number, a digitized image of a handwritten signature that is attached to an electronic message, or merely a name typed at the end of an e-mail message.[4]

III. FOUR LEVELS OF SECURITY

A. First and Second Levels

[9] When entering into a contract online, four degrees of security are possible.[5] The first level would exist if a party accepted an offer by

[1] *See, e.g*, U.C.C. §§ 2-201(1), 2-209(2) (2003).
[2] Thomas J. Smedinghoff, *Electronic Contracts & Digital Signatures: An Overview of Law and Legislation*, 564 P.L.I. PAT. 125, 162 (1999).
[3] Council Directive 1999/93/EC, 2000 O.J. (L 13) 12.
[4] *See* David K.Y. Tang & Christopher G. Weinstein, *Electronic Commerce: American and International Proposals for Legal Structures*, *in* REGULATION AND DEREGULATION: POLICY AND PRACTICE IN THE UTILITIES AND FINANCIAL SERVICES INDUSTRIES 333 (Christopher McCrudden ed., 1999).
[5] Jonathan E. Stern, Note, *The Electronic Signatures in Global and National Commerce Act*, 16 BERKELEY TECH. L.J. 391, 395 (2001).

merely clicking an "I Agree" button on a computer screen.[6] The second level of security would be incurred if secrets were shared between the two contracting parties; this would be exemplified by the use of a password or a credit card number to verify a customer's intention that goods or services were to be purchased.[7]

B. Third Level: Biometrics

[10] The third level is achieved with biometrics.[8] Biometric methods involve a unique physical attribute of the contracting party, and these are inherently extremely difficult to replicate by a would-be cyber-thief.[9] The proposed U.K. identity card would use three types of biometrics: photograph, iris scan, and fingerprints.[10] Other examples are a voice pattern, or a digitized image of a handwritten signature that is attached to an electronic message.[11] In all of these examples, a sample would be taken from the person in advance and stored for later comparison for identification.[12] If a person's handwriting was being used as the biometric identifier, the "shape, speed, stroke order, off-tablet motion, pen pressure and timing information" during signing would be recorded, and this information is almost impossible to duplicate by an imposter.[13]

C. Fourth Level: Digital Signatures with PKI Technology

[11] The digital signature is considered the fourth level of security because it is more complex than biometrics.[14] Many laymen erroneously assume that the digital signature is merely a digitized version of a handwritten signature. This is not the case, however; the digital signature refers to the entire document. The technology used with digital signatures

[6] *Id.*
[7] *Id*.
[8] *Id.*
[9] *Id.*
[10] The Hong Kong government began to issue identity cards several years ago and has been successful with its program. It is a "smart" card with an embedded silicon chip that performs data storage and computational functions. *See*, Rina C.Y. Chung, *Hong Kong's 'Smart' Identity Card: Data Privacy Issues and Implications for a Post-September 11th America*, 4 ASIAN-PAC. L. & POL'Y J. 519, 531 (2003).
[11] Stern, *supra* note 5, at 395-96.
[12] *Id*.
[13] Cyber-SIGN, *The Legality of Electronic Signatures Using Cyber-SIGN is Well Established*, at http://www.cybersign.com/news.htm (last visited Nov. 22, 2004).
[14] Stern, *supra* note 5, at 396.

is known as Public Key Infrastructure, or "PKI."[15] The first step in utilizing this technology is to create a public-private key pair; the private key will be kept in confidence by the sender, but the public key will be available online.[16] The second step is for the sender to digitally "sign" the message by creating a unique digest of the message and encrypting it.[17] The third step is to attach the digital signature to the message and to send both to the recipient. The fourth step is for the recipient to decrypt the digital signature by using the sender's public key.[18] If decryption is possible, the recipient knows the message is authentic, *i.e.*, that it came from the purported sender.[19] Finally, the recipient will create a second message digest of the communication and compare it to the decrypted message digest; if they match, the recipient knows the message has not been altered.[20] Because PKI verifies the source of a message and its contents, digital signatures are the most advantageous type of e-signature.[21]

IV. U.N. LAW OF DIGITAL SIGNATURES AND E-COMMERCE

A. Model Law of Electronic Commerce

[12] The Model Law of Electronic Commerce ("MLEC") was drafted by the United Nations Commission on International Trade Law ("UNCITRAL") and was approved by the U.N. General Assembly in 1996.[22] It is "intended to provide essential procedures and principles for facilitating the use of modern techniques for recording and communicating information in various types of circumstances."[23]

---

[15] Susanna Frederick Fischer, *Saving Rosencrantz and Guildenstern in a Virtual World? A Comparative Look at Recent Global Electronic Signature Legislation*, 7 B.U. J. SCI. & TECH. L. 229, 233 (2001).
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] Jochen Zaremba, *International Electronic Transaction Contracts Between U.S. and EU Companies and Customers*, 18 CONN. J. INT'L. L. 479, 512 (2003).
[21] For an opposing view in favor of biometrics for ordinary transactions, see Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures*, 32 UWLA L. REV. 215, 225-26 (2001).
[22] United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* (1996), *at* http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm (last visited Nov. 22, 2004).
[23] *Id*. at 15, cmt. 13.

[13] Article 7 of the MLEC gives an electronic signature the same legal effect as an ink signature even if "it was not authenticated in a manner peculiar to paper documents,"[24] provided two conditions are met: (1) the signer is identifiable and approved the record and (2) the method used to identify the signer is reliable.[25] Article 7 provides broad guidelines instead of specific prescriptions in order to avoid the "risk of tying the legal framework [of the MLEC] to a given state of technical development."[26] Thus, the MLEC is technologically-neutral.

B. Model Law on Electronic Signatures

[14] Later, UNCITRAL supplemented Article 7 of the MLEC with what became known as the Model Law on Electronic Signatures ("MLES").[27] Pursuant to the MLES, a government agency or a government-approved private firm may use specific types of electronic signatures and serve as a certification authority for that electronic signature.[28] If a government prefers a particular type of electronic signature or technology, then the reliability requirements of MLEC Article 7 must be met.[29] However, this is not intended to exclude other types of technologies which might meet the reliability requirements, but is meant to offer predictability in defining those requirements.[30] The MLES maintains the stance of technological neutrality begun by the MLEC; however, it also attempts to define standards in which specific technologies can be utilized.[31]

V. EU LAW OF DIGITAL SIGNATURES AND E-COMMERCE

A. The EU E-Commerce Directive

[24] *Id*. at 27, cmt. 56.
[25] *Id*. at 6, art. 7.
[26] *Id*. at 27, cmt. 55.
[27] *UNCITRAL Model Law on Electronic Signatures*, [2001] 32 Y.B. U.N. Comm'n Int'l Trade L. 499, U.N. Doc. A/CN.9/SER.A/2001.
[28] *Draft Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures: Note by the Secretariat*, U.N. GAOR, 34th Sess., at 17-18, cmt. 32, U.N. Doc. A/CN.9/493 (2001), *reprinted in* [2001] 32 Y.B. U.N. Comm'n Int'l Trade L. 313, 321-22, cmt. 32, U.N. Doc. A/CN.9/SER.A/2001.
[29] *Id*. at 335, cmt. 133.
[30] *Id*.
[31] *Id*. at 318, cmt. 5.

[15] The EU E-Commerce Directive[32] went into force on July 17, 2000[33] and was required to be implemented by the Member States no later than January 17, 2002.[34] Its major objective is to ensure the free movement of "information society services," *i.e.*, facilitate the growth of e-commerce among the Member States.[35] Member States are required to recognize the legal validity and effectiveness of e-contracts and are precluded from the establishment of obstacles to their utilization.[36] However, the E-commerce Directive is procedural and does not establish substantive rules of international law.[37]

[16] The E-Commerce Directive established the "country of origin" principle: e-businesses of the EU must abide by the national laws of the Member State in which they are established.[38] An e-commerce business is considered to be established in the nation in which it is located.[39] The location of the technical equipment alone will not necessarily be dispositive on this issue.[40]

[17] Article 5 of the E-Commerce Directive requires an e-business to inform consumers of its name, whereabouts, and geographic and electronic mail address.[41] The Directive is not applicable to transactions involving taxation, cartels, gambling, notorial activities, data protection, or intellectual property rights.[42] Member states may specify that the Directive does not apply to situations involving real estate, family law, court documents, or to a promise to pay the debts of another.[43]

[18] The E-Commerce Directive also establishes rules pertaining to the regulated professions, *e.g.*, lawyers and accountants.[44] Online advertising must comply with the respective profession's rules of advertising.[45]

---

[32] *See* Council Directive 2000/31/EC, 2000 O.J. (L 178) 1.
[33] *Id*. at 15, art. 23.
[34] *Id*. at 15, art. 22.
[35] *Id*. at 8, art. 1(1).
[36] *Id*. at 11, art. 9(1).
[37] *Id*. at 8, art. 1(4).
[38] *See* Council Directive 2000/31/EC, 2000 O.J. (L 178) 9, art. 3.
[39] *See id*. at 9, art. 2(c), 3(1).
[40] *Id*. at 9, art. 2(c).
[41] *Id*. at 10, art. 5(1)(a) – (c).
[42] *Id*. at 8, art. 1(5)(a) – (d); *id*. at 9, art. 3(3).
[43] *Id*. at 11, art. 9(2).
[44] *See* Council Directive 2000/31/EC, 2000 O.J. (L 178) 9, art. 2(g).
[45] *See id*. at 11, art. 8.

[19] The E-Commerce Directive provides that messages are deemed sent and received when the parties are able to access it.[46] However, this provision is not applicable to contracts consummated exclusively by electronic means.[47]

B. The EU E-Signatures Directive

[20] In the late 1990s, several European countries began to independently enact digital signature laws pertaining to e-commerce.[48] The EU became concerned because of differences in those laws.[49] In order to provide for a basis upon which to reach convergence, the EU eventually wrote and issued the Directive on a Community Framework for Electronic Signatures ("E-Signatures Directive").[50] All Member States were required to implement it by July 19, 2001.[51] Its main provisions are concerned with legal recognition of electronic signatures, free circulation of electronic signature products, liability, technological neutrality, scope, and international aspects.[52]

C. Legal Recognition of "Advanced" E-Signatures

[21] The E-Signatures Directive distinguishes between basic "electronic signatures" and "advanced electronic signatures."[53] No discrimination is allowed against an electronic signature if it is "advanced," based on a "qualified certificate," and created by a "secure signature creation device."[54] Advanced e-signatures are admissible in legal proceedings[55] and require a greater level of security than basic e-signatures. An "advanced" e-signature is defined to require: a unique link to the signatory; capability of identification of the signatory; creation using means under the sole control of the signatory; and linkage to the data in a manner whereby the recipient is able to detect any alterations to the

[46] *Id*. at 12, art. 11(1).
[47] *Id*. at 12, art. 11(3).
[48] Anthony Burke*, EU and Irish Internet Law: An Overview*, 13 INT'L L. PRACTICUM, at 107, 113-15 (Autumn 2000),
[49] Mariam A. Parmentier, *Electronic Signatures*, 6 COLUM. J. EUR. L. 251, 252 (2000).
[50] Council Directive 1999/93/EC, 2000 O.J. (L 13) 12.
[51] *Id*. at 10, art. 13.
[52] Jacqueline Klosek, *EU Telecom Ministers Approve Electronic Signatures Directive*, 4 CYBERSPACE LAW. 12 (2000).
[53] Council Directive, *supra* note 50, at 5, art. 2.
[54] *Id.* at 7, art. 5.
[55] *Id.* at 7, art. 5(1)(b).

original document sent by the signatory.[56]

D. CSP Requirements and Liability

[22] The E-Signature Directive also provides for explicit requirements for qualifying as a Certification Service Provider ("CSP").[57] A CSP is an independent party that provides qualified certificates, electronically attesting that an electronic signature is linked to a particular person.[58] All "electronic-signature products" of CSPs must be allowed to circulate freely, subject only to the laws of the country of origin.[59] The E-Signature Directive places much reliance on CSPs to ensure that a requisite level of security is maintained. Accordingly, CSPs are held liable for damages suffered by any entity or person who reasonably relies on a qualified certificate.[60]

E. Technological Neutrality

[21] The E-Signature Directive does not explicitly require the use of any specific technology; ostensibly, it is technologically neutral.[61] However, because of its emphasis on attainment of security, the Directive does seem to implicitly support the use of more sophisticated and security-minded technologies, such as PKI.

F. Scope

[22] The E-Signatures Directive was intended to have a narrow scope,[62] and was not intended to affect the validity of contracts generally, nor meant to modify the formation requirement established by national or EU contracts law.[63] In other words, it is procedural and does not establish any substantive contract law.[64]

G. International Aspects

[56] *Id.* at 5, art. 2(2) (a)-(d).
[57] *Id*. at 11, Annex II(d).
[58] *Id.* at 11, Annex II.
[59] Council Directive, *supra* note 50, at 7, art. 4(2).
[60] *Id.* at 7, art. 6.
[61] Klosek, *supra* note 52, at 12.
[62] Council Directive, *supra* note 50, at art. 1.
[63] *Id*. at 5, art. 1.
[64] *See generally id.*

[23] The Directive encouraged the development of e-commerce on a global scale by requiring cooperation in the recognition and acceptance of qualified certificates issued by CSPs located outside the EU, provided that the foreign CSP fulfills the requirements established in the E-Signatures Directive.[65] This international application of the E-Signatures Directive distinguishes it from the EU E-Commerce Directive, which does not have international application.[66]

VI. U.K. LAW OF DIGITAL SIGNATURES AND E-COMMERCE

A. Electronic Signatures Regulations 2000 and Electronic Communications Act 2000

[24] The U.K. Electronic Signatures Regulations 2000 ("E-Sign Regulations") went into force on March 8, 2002.[67] The purpose of E-Sign Regulations is to implement certain provisions of the EU E-Signatures Directive, most notably the provisions pertaining to Cryptography Service Providers ("Cryptography SPs"), including liability and data protection.[68] On May 25, 2000, the U.K. Electronic Communications Act 2000 ("ECA") was enacted.[69] It provided that responsibility for the establishment of a register of approved Cryptography SPs lies with the Secretary of State.[70]

[25] The U.K. adopted the same definitions as the EU E-Signatures Directive for "e-signature," "e-signatory," and Cryptography SP.[71] Legal persons can be signatories, but no definition was provided for "secure signature creation device."[72] The same two types of signatures ("Basic" and "Advanced") were adopted by the U.K. as in the EU E-Signatures Directive.[73] Since U.K. law does not distinguish the concept of "handwritten" signature, it was not necessary to specifically recognize an

[65] *Id*. at 8, art. 7(1)(a).
[66] *Id*. at 9, cmt. 58.
[67] Interdisciplinary Centre for Law & Info. Tech., Katholieke Universiteit Leuven, *Study for the European Commission: The Legal and Market Aspects of Electronic Signatures*, 215-16 (2003) [hereinafter *Legal and Market Aspects*].
[68] *Id.* at 215.
[69] Electronic Communications Act, 2000, c.7 (Eng.).
[70] *Id.* at c.7, s.1.
[71] *Legal and Market Aspects*, *supra* note 67.
[72] *Id.*
[73] *Id.*

"e-signature" as an alternative to a handwritten one.[74] However, "various [U.K.] legislative acts have generally recognized [sic] that an e-signature is a valid form of signature in the specific context concerned."[75]

[26] The ECA "addresses the admissibility but not the legal effectiveness" of an e-signature.[76] Legal effectiveness is "generally addressed through specific Orders" of a court, and they are "generally valid in the absence of specific legislation" to the contrary.[77] E-signatures are admissible as evidence in court, but their probative value is to be decided by the court on a case-by-case basis.[78] In some special situations, e-signatures may be prohibited.[79]

[27] The E-Sign Regulations adopted the same grounds for liability of Cryptography SPs as in the EU E-Signatures Directive.[80] However, the E-Sign Regulations established a "[r]everse burden of proof," with "[n]o express liability limitations as in the Directive."[81] Thus, tort rules of proximate causation apply.[82]

[28] The E-Sign Regulations provide for data protection obligations of the Cryptography SP only.[83] Enforceability clauses are included and the scope of their applicability is explained.[84] Although specific data protection restrictions for Cryptography SPs are included, no specific reference is made to the U.K. Data Protection Act.[85]

VII. U.S. LAW OF DIGITAL SIGNATURES AND E-COMMERCE

A. U.S. Model State Law: The UETA

[29] After e-commerce began to develop in the 1990s, U.S. states began

[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Legal and Market Aspects*, *supra* note 67.
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] *Legal and Market Aspects*, *supra* note 67.
[84] *Id.*
[85] *Id.*

to enact laws to regulate it.[86] In an effort to move toward uniformity in these laws, the U.S. National Conference of Commissioners on Uniform State Laws ("NCCUSL") created the Uniform Electronic Transactions Act ("UETA"),[87] a model law. Since its creation, the UETA has been adopted in almost all U.S. jurisdictions, either in its original form or with amendments.[88]

1. Purpose

[30] The purpose of the UETA is to facilitate e-commerce by giving electronic records and agreements the same legal status as "hard" copy records and agreements. Like the EU Directive and its U.S. federal counterpart, E-Sign, UETA is procedural and does not affect the substantive law of contracts.[89]

2. Section 7: The Centerpiece

[31] The heart of the UETA is found in section 7, which states:

> A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
> A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
> If a law requires a record to be in writing, an electronic record satisfies the law.
> If a law requires a signature, an electronic signature satisfies the law.[90]

[32] The UETA's definitions of "transaction,"[91] "electronic,"[92] "electronic record,"[93] and "electronic signature"[94] are broadly worded and inclusive.

---

[86] Ian A. Rambarran, *I Accept, But Do They?: The Need for Electronic Signature Legislation on Mainland China*, 15 TRANSNAT'L LAW. 405, 417-18 (2002).
[87] UNIF. ELEC. TRANSACTIONS ACT, 7A U.L.A. 23 (2002 & Supp. 2004).
[88] Christopher William Pappas, *Comparative U.S. & EU Approaches to E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures and Taxation*, 31 DENV. J. INT'L L. & POL'Y 325, 341 (2002).
[89] *Id.*
[90] UNIF. ELECTRONIC TRANSACTIONS ACT, 7A U.L.A. 252 (2002).
[91] *Id*. § 2(16), at 227.
[92] *Id*. § 2(5), at 226.
[93] *Id*. § 2(7), at 226.
[94] *Id*. § 2(8), at 226.

3. Exclusions

[33] The UETA provides for several "safe havens" which escape its coverage. The UETA does not apply to: (1) wills and trusts;[95] (2) transactions that are covered by the Uniform Commercial Code ("UCC"), other than documents invoking Section 1-107 and 1-206, Article 2 and Article 2A;[96] (3) the Uniform Computer Information Transactions Act ("UCITA");[97] and (4) other laws to be identified by the states.[98]

4. Attribution; Sworn Statements

[34] The UETA's attribution procedures are used to decide whether an electronic record or an electronic signature can be legally linked to a person or entity.[99] Section 9(a) of the UETA maintains that an electronic record or signature can be attributed to a party if it is the result of that party's actions.[100] The UETA disposes of the notarization requirement by simply stating that an electronic record satisfies that requirement if it is attached or logically associated with the signature or record of the person authorized to sign the record.[101]

5. Use of Electronic Agents; Admissibility; Technological Neutrality

[35] Under the UETA, it is perfectly acceptable for a contract to be entered into through the use of an electronic agent. This is allowed even though no person was aware of the electronic agent's action or the resulting contract.[102] In any legal proceeding, "evidence of a record or signature may not be excluded solely because it is in electronic form."[103] The UETA is "technologically neutral" and does not give any preference to more sophisticated or more secure technologies, such as PKI.[104]

6. Electronic "Mailbox Rule"

[95] *Id*. § 3(b)(1), at 235.
[96] UNIF. ELECTRONIC TRANSACTIONS ACT § 3(b)(2), 7A U.L.A. 252 (2002).
[97] *Id*. § 3(b)(3), at 235.
[98] *Id*. § 3(b)(4), at 235.
[99] *See id*. § 9, at 261.
[100] *Id*. § 9(a), at 261.
[101] *Id*. § 11, at 266.
[102] UNIF. ELECTRONIC TRANSACTIONS ACT § 14(1), 7A U.L.A. 252 (2002).
[103] *Id*. § 13, at 271.
[104] Rambarran, *supra* note 86, at 419-20.

[36] An electronic message will be considered "sent" when it is properly addressed or directed through an information processing system pursuant to the instructions of the recipient.[105] An electronic message will be considered "received" when it enters a previously designated information processing system and is capable of being retrieved by the recipient.[106] For example, if a business agreement is to be formed via e-mail, a contract will come into existence at the moment the offeree sends a message of acceptance to the offeror at the e-mail address provided to the offeree by the offeror. The contract will exist as soon as the acceptance could have been retrieved by the offeror, notwithstanding that the offeror has not yet read the message of acceptance. This is similar to the impact of the traditional "mailbox rule."[107]

7. Transferable Records

[37] Finally, the UETA effectively supplements the UCC. Under the UETA, negotiable instruments (promissory notes under UCC Article 3, and other documents under UCC Article 7) are considered to be "transferable records" when in electronic form.[108]

B. U.S. Federal Law: E-Sign

[38] The UETA was drafted in hopes of achieving a degree of uniformity in e-commerce law among the states.[109] In order to motivate states to adopt e-commerce laws which fully comported with the UETA, and to ensure that all states recognized the validity of contracts entered into electronically, the U.S. Congress passed the Electronic Signatures in Global and National Commerce Act,[110] popularly referred to as "E-Sign." It was promptly signed into law by President Clinton and it became effective on October 1, 2000.[111] E-Sign has more commonalities with the UETA than it has differences. E-Sign, like the UETA, is procedural in

[105] UNIF. ELECTRONIC TRANSACTIONS ACT § 15(a)(1), 7A U.L.A. 274 (2002).
[106] *Id*. § 15(b), at 274-75.
[107] For an explanation of the "mailbox rule", see 2 SAMUEL WILLISTON, WILLISTON ON CONTRACTS § 6:32 (Richard A. Lord ed., 4th ed. 2001).
[108] UNIF. ELECTRONIC TRANSACTIONS ACT § 16, 7A U.L.A. 279 (2002).
[109] *See* S. CONF. REP. NO. 106-76, at S5282 (2000).
[110] Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7031 (2000).
[111] Amy J. Dunn, *Survey of Legislation: Uniform Electronic Transactions Act*, 24 U. ARK. LITTLE ROCK L. REV. 603, 612 (2002).

nature and does not replace the substantive law of contracts.[112] E-Sign also recognizes the legal validity of electronic contracts[113] and electronic signatures.[114] It provides for legal recognition of transferable records which are in electronic form.[115]

1. Similarities to the UETA

[39] E-Sign provides for legal recognition of contracts which are formed exclusively though use of electronic agents.[116] It gives a party the legal right to demand a "hard" copy instead of being forced to accept an electronic copy.[117] And, E-Sign, like the UETA, is not applicable to wills and instruments covered under the UCC (other than UCC Sections 1-107 and 1-206 and Articles 2 and 2A).[118] Furthermore, E-Sign continues the tradition of technological neutrality which was adopted in the UETA.[119] No particular form of technology, such as PKI or biometrics, receives any favoritism or preference; an open mind is maintained toward all of them. Finally, E-Sign's definitions of "electronic,"[120] "electronic signature,"[121] and others are as broadly worded and inclusive as UETA's definitions.

2. Departures from the UETA

[40] However, E-Sign is not a clone of the UETA. For example, E-Sign does not contain anything analogous to the mailbox rule, as the UETA does.[122] Furthermore, E-Sign lacks any guidelines for attributing an electronic signature to an individual.

[112] Benjamin Suksomnil, *An Analysis of the Electronic Signatures in Global and National Commerce Act and Its Effects on E-Commerce and the Online Consumer*, 2002 SYRACUSE L. & TECH. J. 2, § V (2002).
[113] 15 U.S.C. § 7001(a).
[114] *Id*.
[115] *Id*. § 7001(b)(1).
[116] *Id.* § 7001(h).
[117] *Id.* § 7001(b)(2).
[118] *Id.* § 7003(a)(1), (3). E-Sign also does not apply to: (1) judicial documents; (2) creditor proceedings; and (3) certain documents pertaining to the transportation of hazardous materials. *Id.* § 7003(b)(1), (2)(B), (3).
[119] Suksomnil, *supra* note 112, §§ V, VI.
[120] 15 U.S.C. § 7006(2).
[121] *Id.* § 7006(5).
[122] *See* Suksomnil, *supra* note 112, § V.

3. Consumer Protections

[41] The most significant and dramatic difference is E-Sign's inclusion of consumer protection provisions.[123] The U.S. Congress was very concerned with ensuring that consumer rights were recognized and maintained in e-commerce law.[124] Under E-Sign, any law that requires information relating to a transaction to be provided to a consumer will be satisfied with an electronic record if: (1) the consumer affirmatively consents after being provided with a clear and conspicuous statement informing the consumer of her rights and obligations;[125] (2) prior to consenting, the consumer is notified of her right to withdraw consent and the procedure for doing so;[126] (3) the consumer consents electronically in such a manner that demonstrates that the consumer can access the information that is the subject of the consent;[127] and (4) after consenting, the consumer is provided with a statement pertaining to any changes in the software or hardware necessary to access the information that the consumer originally consented to and must be allowed to withdraw her consent without cost.[128] Notwithstanding the above, a contract entered into by a consumer cannot be denied legal effect for the sole reason that disclosures were given in electronic form without the consumer's consent.[129] Furthermore, E-Sign does not affect the content, timing or location of any required disclosures.[130]

4. The Preemption Clause and its Undesirable Result

[42] Pursuant to E-Sign's Preemption Clause, E-Sign will preempt any state law that addresses the same issues as E-Sign, unless:(1) the state has adopted the UETA in its *original* form, without modification;[131] or (2) the state has adopted other procedures or requirements which are consistent with E-Sign pertaining to electronic records and electronic signatures in e-commerce.[132]

---

[123] 15 U.S.C. § 7001(c); Jamie A. Splinter, Comment, *Does E-Sign Preempt the Illinois Electronic Commerce Security Act?*, 27 S. ILL. U. L.J. 129, 135 (2002).
[124] *See* S. CONF. REP. NO. 106-76, at S5282-83 (2000).
[125] 15 U.S.C. § 7001(c)(1)(A)-(B).
[126] *Id.* § 7001(c)(1)(B)(i)(II), (iii).
[127] *Id.* § 7001(c)(1)(C)(ii).
[128] *Id.* § 7001(c)(1)(D)(i).
[129] 15 U.S.C. § 7001(c)(3).
[130] *Id.* § 7001(c)(2)(A), (f).
[131] *Id.* § 7002(a)(1).
[132] *Id.* § 7002(a)(2)(A)(i).

[43] In adding the preemption clause to E-Sign, the U.S. Congress attempted to achieve uniformity in e-commerce law pertaining to electronic records and signatures.[133] Unfortunately, that aspiration has not been realized. The preemption criteria are murky and vague; it is not at all clear-cut as to when E-Sign will preempt state law and when it will not. The U.S. is left with a "patchwork quilt" of non-uniform state laws applicable to e-commerce.[134]

VIII. Three Categories of Digital Signature Laws

[44] Many countries have now adopted some form of digital signature law. These laws may be grouped into three categories.

A. Prescriptive Law

[45] Countries that have adopted these laws have mandated PKI technology for use in digital signatures.[135] This category includes Germany, Italy, Malaysia, and Russia.[136] Unlimited liability may be imposed for negligent loss of a private key resulting in loss or damage.[137]

B. Hybrid Model

[46] Hybrid laws are more market-driven.[138] Examples are the EU Directive, the U.N. Model Law, Singapore (with an e-signature law resembling the U.N. Model Law), and Bermuda.[139] These laws have "limited technological neutrality."[140] However, if the specified

---

[133] *See* S. CONF. REP. NO. 106-76, at S5282 (2000).

[134] One commentator, Ms. Celeste May, noted that,

> There are basically two schools of thought out there [on preemption]…. One is that if you change anything in the NCCUSL version of UETA then all of the bill would be subject to federal preemption by E-Sign. The other school of thought is that if that if you change it, then only that section that has been changed will be subject to preemption under federal law.

Nathan A. Huey, Note, *E-Mail and Iowa's Statute of Frauds: Do E-Sign and UETA Really Matter?*, 88 IOWA L. REV. 681, 696 n.80 (2003).

[135] Fischer, *supra* note 15, at 234.

[136] *Id.*

[137] *Id*.

[138] *Id.* at 235.

[139] *Id.*

[140] *Id.* at 236.

requirements are met, "certain favored technologies are afforded special presumptions, such as a presumption of authenticity."[141] The only existing technology that appears to meet the requirements of the EU Directive's "advanced electronic signature" is PKI.[142] The hybrid model allows CSPs to limit their liability by specifying limitations on the qualified certificate.[143] Hybrid models purport to be more flexible and adaptable to new technological developments, while simultaneously building public trust in digital signatures.[144]

C. "Minimalist" Laws

[47] Countries with minimalist laws are extremely market-oriented and permissive.[145] Most common law jurisdictions of the world have adopted this approach, including the U.K., U.S., Australia, and New Zealand.[146] Minimalist laws are completely technology-neutral.[147] For example, the U.S. E-Sign and the UETA "provide that [] no electronic signatures of whatever type may be denied legal effect … because it is [sic] in electronic form. No special presumptions are given to PKI, or to any other particular technology."[148] Critics of the minimalist approach contend that it is too vague and creates too much legal uncertainty.[149]

IX. CONCLUSIONS AND RECOMMENDATIONS

[48] 1. The U.K. and U.S. are too "minimalist" and need to achieve more stringency and standardization in their e-signature laws. The European Union took a hybrid approach and has provided a model worthy of emulation by the U.K., U.S., and other "minimalist" countries. Although not requiring the utilization of a specific technology, the EU Directives do place "advanced" e-signatures on a pedestal, and the only technology currently able to meet the "advanced" requirements is PKI. Therefore, the EU, by defining the "advanced" e-signature so stringently, has called for the utilization of PKI, by implication, while keeping an open mind to new technologies that will undoubtedly become available in the future.

[141] Fischer, *supra* note 15, at 236.
[142] *Id.* at 237.
[143] *Id.* at 236.
[144] *Id.*
[145] *Id.* at 237.
[146] *Id.* at 236-37.
[147] Fischer, *supra* note 15, at 237.
[148] *Id.*
[149] *Id.*

[49] 2. The European Union has also provided high standards for Certification Service Providers. These standards, or legally equivalent ones, need to be implemented globally. To illustrate the importance of this, consider the following situation. If a U.S. firm is engaged in a business transaction with an EU firm, and is required to comply with EU law, the U.S. firm should use an advanced e-signature instead of a basic one. Furthermore, the advanced E-signature should be based on a qualified certificate created by a CSP, and all of the certification requirements in the U.S. must be legally equivalent to those in the EU.

[50] 3. The "patchwork quilt" of e-signature laws in the United States is a mess. It needs to be replaced with a national law applicable to all fifty states. E-Sign in its present form is a failure. E-Sign's preemption clause creates an uncertain, vague, and unpredictable situation in which no one can be sure just what the law is. The U.S. Congress should quickly "clean up" the mess by mandating, in no uncertain terms, E-Sign's preemption of all existing state laws currently in effect. In addition to the attainment of uniformity, another beneficial outcome would be the imposition of the consumer protection provisions which are a distinguishing aspect of E-Sign, and which were held in high regard by the Congress when it wrote E-Sign.

X. TWO FINAL THOUGHTS: TRUST AND THE ENDLESS QUEST

[51] The adoption of high standards of internet security with digital signatures and other cutting-edge technologies will lead to more trust and confidence in the integrity of the process, which, in turn, will promote growth in e-commerce. Scott Lowry, CEO of a U.S. Certification Authority, observed:

> For people to truly leverage the power of the Internet, they must have the same level of confidence in an online relationship as they do when meeting in person … [Digital signatures are] security tools that are backed by stringent policies and procedures allowing people to trust the authenticity and enforceability of electronic transactions.[150]

[150] Press Release, Digital Signature Trust, Digital Signature Trust Becomes Licensed as Certification Authority in Texas (May 16, 2001) (WESTLAW, PR Newswire).

[52] However, there is a *caveat*. The search for more secure e-commerce methods is never-ending. Benjamin Wright, a Texas attorney and author, noted that no procedures pertaining to paper-and-ink signature requirements, biometric procedures, or even digital signatures utilizing PKI, can provide a guarantee of document authenticity and security: "*The development and use of authentication technology is a dynamic process. It is not a destination; it is an endless journey in which the good people hurry to stay a step or two ahead of the bad people*."[151]

[151] Wright, *supra* note 21, at 225 (emphasis added).