Law and Business Review of the Americas

Volume 7 | Number 3 Article 7

2001

Why Electronic Signatures Can Increase Electronic Transactions and the Need for Laws Governing Electronic Signatures

Sarah Wood Braley

Why Electronic Signatures Can Increase Electronic Transactions and the Need for Laws Governing Electronic Signatures

*Sarah Wood Braley**

Table of Contents

* Sarah Wood Braley is a 2002 J.D. candidate at Southern Methodist University Dedman School of Law, Dallas, Texas. This article is an adaptation from a comment presented by Ms. Braley as a member of the International Law Review Association of SMU (ILRA). As a member of the ILRA, Ms. Braley served as Symposium Editor.

I. Introduction

This article addresses the need for laws governing electronic signatures. Although many countries have begun to address this need, there is still uncertainty as to what the final outcome will be. There is also a question as to whether countries will keep working to redraft model laws and if such model laws will be enacted.

The need for laws governing electronic signatures comes from the benefits that electronic transactions can provide not only to individual transacting parties, but also to the world economy as a whole. However, without uniform laws governing electronic signatures transacting parties are not taking full advantage of electronic transactions. This is due to transacting parties' fear of authenticity, integrity, confidentiality, repudiation, and reliability.[1] Three scenarios are outlined in this article that demonstrate why and how these fears are created. In addition, this article provides an in-depth description of how electronic signatures work and how they will confront the fears of electronic transactions.

Electronic signatures can address many of these fears in electronic transactions. There is, however, one fear that electronic signatures themselves cannot address, reliability; the fear that electronic transactions will not be considered valid under current law in different countries and jurisdictions throughout the world. This article suggests that transacting parties will not fully utilize electronic commerce until lawmakers help create reliability in the electronic transaction process by recognizing the validity of electronic signatures as compared to handwritten signatures.

This article suggests five general considerations that lawmakers should consider and evaluate when legislating electronic signatures: (1) evidentiary value; (2) technology preference; (3) intent of parties; (4) preference between signature types; and (5) international compatibility. In conclusion, this article takes a brief look at three enacted or pending laws governing electronic signatures (UNCITRAL, EU, and E-Sign) and compares the three laws with the five considerations laid out above.

II. Electronic Transactions

It has quickly become the norm for people all over the world, from governments to sophisticated businesspeople to unsophisticated consumers, to conduct electronic transactions and contracts over the Internet. Governments, businesspeople, and consumers have begun to realize the immense advantages the Internet can offer. Time, money, and hardship can be saved on both sides of transactions. This is due to the increased speed of transmitting information, using less paper, and the ability to conduct face-to-face

1. Reliability in the sense that parties can rely on their contract being legally enforceable.

transactions without leaving your home or office. Profits can increase not only because transacting parties are saving time and money, but also because global consumer markets are now just a "point and click" away.

Economically, the Internet has just begun to have a positive effect on global economic growth. Because electronic commerce and electronic administration is rapidly advancing, many countries and governments across the world are realizing the challenge of moving to a paperless society. Governments, businesspersons, consumers, and lawyers are beginning to recognize the legal problems arising from electronic commerce. A major problem that has begun to be addressed in many countries is the validity of electronic transactions as they relate to valid, enforceable, and reliable contracts.

Consumers might not realize that the last time they ordered a book on Amazon,[2] placed a bid for a rare baseball card at an eBay[3] auction, or bought flowers from an Internet florist that they were entering into a contract with the respective "dot com" company. These consumers might be bound when they click on the "accept terms and conditions" box instead of signing a contract. Businesspeople might not realize that the negotiations they conduct via email could be considered valid offers and acceptances and, thus, binding contracts even though neither party actually signed a piece of paper.

The converse may also be true depending on what country, state, or jurisdiction you are in. For example, ordering a consumer product over the Internet might not be a binding contract. This especially creates problems when the consumer or businessperson does not know whom he or she is dealing with; it is just a name on the screen. There are no "real" people to talk with, no stores to go visit, and no managers to complain to. Furthermore, emails might not be considered valid offers and acceptances for consumers and businesspeople even when the parties initially intended them to be valid.

Consumers and businesspeople can also have problems when individuals other than themselves enter into online transactions using their information. For instance, this can happen when a colleague uses your computer to send an e-mail message and the receiving party thinks the e-mail is from you. If the message were in the form of an offer or acceptance, would it be considered valid? This could also happen when a friend jokingly enrolls you in the "Barbie Doll Fan Club" when you are a thirty-year-old male with no interest in Barbie dolls. If the form your friend filled out, in your name, looked like a contract and he accepted the "terms and conditions" of the fan club, including paying club dues in the future, would this be considered a valid contract? No one quite knows the answer.

The legal uncertainty of parties' actions and dealings in cyberspace leave parties on both ends of transactions in a confused state. Confusion in the law is never a good thing. This allows for some parties to take advantage of the system because they realize there are no prescribed consequences for potentially wrongful actions. When there are no defined rules, parties cannot anticipate and protect themselves from possible problems. This in turn makes parties afraid to conduct electronic transactions for fear they may be taken advantage of. The consequence is a circular effect of parties unwilling to engage in the great resource of the Internet.

2. http://www.amazon.com.
3. http://www.ebay.com.

A. IDENTIFIED PROBLEMS

Currently one can identify three common scenarios that are examples of why the full benefits of electronic transactions are not being taken advantage of.[4]

1. Scenario One: Untrusting Party

In the "untrusting party" scenario, parties are too skeptical of the authenticity, integrity, confidentiality, and reliability[5] of electronic transactions to even enter into them. When addressing authenticity, parties are untrusting of who is actually on the other end of the screen. There is an understandable fear that the person, identity, or company that one is conducting business with is not who they purport to be. Parties want to make sure that "a communication purported to be from a particular person is in fact from that person and is not a forgery."[6] There is no guarantee that after you type in your credit card number and send your check or goods that you will be able to contact that company or individual tomorrow. There is a sense of hidden identity on the Internet that reasonably makes parties doubtful of the full advantages of the Internet.

As for integrity, parties are afraid of what happens to their message, document, order, or other transaction after he or she sends it. Parties want to ensure "that the communication is complete and accurate without it having been altered in any way during transmission or storage."[7] There is no guarantee that a third party will not intercept the message and change its contents. The reverse is also true. The receiving party cannot be guaranteed that he or she is receiving the same message that was originally sent.

Equally important are parties' fear of confidentiality. Just as with any form of communication, be it mail or telephone conversation, people want their communications and transactions to be confidential. On the Internet, there is no assurance that a third party cannot intercept your message, read it, and retain important information. This fear affects everyone from governments relying on top secret information, to businesspeople conducting confidential transactions, to consumers entering their credit card number. Some parties are justifiably unwilling to give up confidentiality for the increased benefits of the Internet.

Finally, there are parties' fears of reliability. This problem comes in two forms and again causes parties not to use the Internet for commercial transactions. First, parties are not sure how electronic transactions apply to current law and are unwilling to divert from the trusted written and signed contract for fear that the contract will not be upheld in a court of law.[8] Second, parties are not assured that the other party will not repudiate their willingness to be bound to the transaction. They want to "rule out the possibility of the sender of the communication denying that it was sent or sent in the form in which it

4. The author, from interviews and observations, developed these three scenarios. They do not purport to be complete reasons for why individuals do not use the Internet, just three common examples.
5. Later in the article the term "reliability" will be combined with the term "nonrepudiation."
6. P. P. Kanthan, *Legal Aspects of Electronic Commerce and the Scope for Appropriate Legislation*, 4 CYBER. LAW. 24, 25 (2000).
7. *Id.*
8. This problem comes into play especially when dealing with the Statute of Frauds or similar regulation.

was received by the recipient."[9] There is no recognized way to prove that parties intended to be bound as there is with a written contract and signature. Offers and acceptances over the Internet are in different forms than we have seen in the past.

For example, in electronic data interchange "contractual offers and acceptances are exchanged without conscious human intervention at the time of the exchange."[10] A receiving computer is programmed to accept an offer by sending an acceptance message back to the offeror when the terms of the offer match the acceptance program.[11] Situations like these raise questions as to whether or not the parties can be bound to the computer's programs. Similarly, an offeree or offeror may be able to deny his or her offer or acceptance when conducting transactions via email. An accepting party may try to deny his acceptance by claiming that he did not read the "terms and condition" box or did not understand the legal significance of pressing the "acceptance" box and replying to the email.[12]

In scenario one, when contracting parties do not enter into commercial transactions because they are worried about authenticity, integrity, confidentiality, or reliability the full benefits of electronic transactions are lost because parties never begin to use the advantageous technology that is available. In the next two scenarios, parties enter into electronic transactions, but then one of two problems arises that do not allow parties to maximize the advantages of the Internet.

2. *Scenario Two: Partially Trusting*

In the "partially trusting" scenario, parties negotiate through all of the normal transaction steps electronically[13] until it comes to executing the last step—showing their intent to be bound to the transaction. Then, one or both of the parties get skeptical and have to revert to the old transaction methods—sending written documents and requiring written signatures. Parties again may be afraid of authenticity, integrity, confidentially, or reliability.[14]

In this scenario, the full benefits of electronic transaction are not lost. It is only in the last step where the parties do not maximize time and cost efficiency by having to revert to sending their documents via mail. However, this is still a transaction cost that could have been avoided.

3. *Scenario Three: Unfortunately Trusting*

In the "unfortunately trusting" scenario, there are parties who are not skeptical of electronic transactions and complete all transaction steps electronically, including showing their intent to be bound to the transaction. These parties are not afraid of

9. Kanthan, *supra* note 6, at 25.
10. henry h. perritt, Jr., Law and the Information Superhighway, 376 (John Wiley ed., 1996).
11. *See id.*
12. *See id.*; *see also id.* at 376–77 (for other examples of common problems).
13. Examples of "normal" transaction steps: offers and possible acceptance via email, electronic data interchange, or filling in contract forms electronically and making negotiated changes via email.
14. *See supra* Part II.A.1.

authenticity, integrity, confidentially, or reliability.[15] They have either confidence or ignorance in the system.

Unfortunately, one party decides he does not want to be bound to the transaction and tries to get out of his agreement by questioning the validity of his agreement because it was conducted electronically. This problem arises because there are no uniform and accepted customs for dealing with ways to bind parties to their electronic transactions. The breaching party most likely realizes that there are no predetermined legal consequences to his actions and, therefore, "uses" the system to get out of the contract for any number of reasons. In this scenario, the full benefits of electronic transactions will be lost due to the time and cost of resolving the conflict and ultimately the lost opportunity of the intended transaction.

In all three scenarios, the benefits of electronic transactions are lost either because people are afraid of the protection systems in place or because people are taking advantage of the systems in place. There is a need to provide a system that gives users authenticity, integrity, confidentiality, and reliability.

If a uniform or semi-uniform body of law is developed governing aspects of electronic transactions, parties will be able to have confidence in the technology. Only then will the three scenarios discussed above begin to be addressed. Parties will be more willing to not only use electronic transactions, but they will complete their transactions electronically. Furthermore, there will be protection from those who take advantage of the current unsureties governing electronic transaction.

B. An Age-Old Problem

Although the ideas and problems behind electronic transaction may be somewhat new, they still can be reduced to contract basics. One of the basics is the need to authenticate and validate the transaction parties enter into over the Internet. This fundamental problem "goes back 350 years to the adoption of the Statute of Frauds in England in 1677."[16] At that time, there was an idea that there should be a "formal recognition between contracting parties of the making of and existence of their contractual relationship."[17] Historically, this is what written contracts and signatures have come to provide—trustworthy proof that each party intended to be bound to the transaction and all its terms. The purpose of the Statute of Frauds was the preference of the "reliability of written evidence of contract rather than the fallibility of memory of oral statements."[18]

Lack of a legally cognizable way to sign, authenticate, and validate electronic transactions is a primary obstacle facing the contracting process in cyberspace today. For example, the Uniform Commercial Code (UCC) of the United States requires that every

15. *Id.*
16. Richard Allan Horning, *Legal Recognition of Digital Signatures: A Global Status Report*, 22 Hastings Comm. & Ent. L.J. 191, 192 (2000).
17. *Id.*
18. perritt, *supra* note 10, at 553.

contract for the sale of goods in excess of $500 or more be in writing and be signed.[19] Similarly, the United States Copyright Act requires that a copyright assignment "be in writing and signed by the copyright holder."[20] These examples show that there is a need for contracting parties to check the relevant statutes and jurisdictions to see if their electronic transactions will be considered valid. Unfortunately, this process can take time and money, which some parties are unwilling to invest especially when large sums of money are concerned.[21] Parties will, therefore, continue to contract through the reliable old methods[22] and waste the advantageous technology that is available to them.

C. What Is Needed?

If the world is to take full advantage of the ability to conduct electronic transactions, then there needs to be an advanced and partially uniformly-accepted electronic way to provide "trustworthy proof" that parties intended to be bound to their transactions. However, "[p]aper documents can only be replaced by purely electronic documents where the latter bear authentication devices, which are functionally equivalent to manual signatures."[23] This is because parties are afraid to divert from trusted and legally recognized written signatures. As one president of an e-commerce company said, "[e]nd users are suspicious of technology, especially when it replaces such a fundamental component[24] of our social fabric."[25]

Currently, there is an imminent need to authenticate an electronic document in the same way that a written signature authenticates a "paper"[26] document. This is where a partially uniform and accepted body of law governing electronic signatures can step in. Although the term "electronic signature" has many different definitions,[27] basically it is a "software-driven method of authenticating the origin and integrity of an electronic message."[28] In other words, it is a way to provide trustworthy proof of the party's intent

19. U.C.C. §2–201 (1977). "Except as otherwise provided in this section a contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker." *Id.* §2–201(1).
20. david johnston et al., cyber law: what you need to know about doing business online, 179 (1997).
21. *See id.*
22. Referring to written contracts with written signatures delivered either in person or via mail.
23. Miriam A. Parmentier, *Legislative Development: Directive 1999/93 on a Community Framework for Electronic Signatures*, 6 Colum. J. Eur. L. 251 (2000).
24. Meaning handwritten signatures.
25. *E-Sign Only First Step Towards True E-Commerce*, Computer Security Update, Aug. 2000, *available at* http://www.silanis.com/news/press_room/press_releases.html (quoting Tommy Petrogiannis, President of Silanis Technology).
26. Meaning handwritten or typed pieces of tangible paper.
27. *See* W. Everett Lupton, *The Digital Signature: Your Identity by the Numbers*, 6 Rich. J. L. & Tech. 10, 11–12 (1999).
28. John Dickie, Internet and Electronic Commerce Law in the European Union 35 (1999).

to be bound to the transaction and its terms; just as written signatures do.[29] Electronic signatures will be able to take on all the positive attributes of written signatures and maybe more. This is because electronic signatures act like an "identification mark covering the entire document and [are] therefore unique to every document."[30] This can be analogized to initialing every sentence of a contract.

III. Electronic Signatures

A. How Electronic Signatures Work

Electronic signatures use a technology called encryption. The basic idea of encryption is to take an original written message through a computer program and translate that original written message into unreadable computer code. Computer software does this by employing one or more different technologies. The message is then transferred to the receiving computer that again employs technologies and transfers the unreadable message back to the original message sent.[31]

In order to fully understand electronic signatures it is necessary to define some terms and go beyond the basic idea.[32] First, "*[c]ryptography* is a process by which data (which could be anything from a text email message, to a digital picture, to a binary software program, to streaming dated of a real-time digital phone conversation) is kept secret by scrambling it so as to render it unintelligible gibberish"[33] to an outside party. The original message sent is called "*plaintext*"[34] and the "disguised message is called a *ciphertext*."[35] The process of converting the original message (plaintext) into the disguised message (ciphertext) is called *encryption*.[36] Conversely, the process of converting the ciphertext into plaintext is called *decryption*.[37] One of the important tools used to convert the text is called an algorithm, which is a "mathematical function used to encrypt and decrypt a message"[38] using a key. A key needs to be used because it can be kept secret between the transmitting parties, whereas algorithms most likely cannot.[39]

The question arises, why do our "keys" need to be kept secret? One answer is that there are people who are trying to intercept and read messages that are intended only

29. It is important to note that electronic signatures are not necessarily the reproduction of the sender's written signature as it would appear on a piece of paper.
30. Kanthan, *supra* note 6, at 25.
31. See perritt, *supra* note 10, at 392–96; *see also* johnston, *supra* note 20, at 93–94.
32. The author feels that encryption technology will soon be the norm and it is important for readers to move beyond basic understanding of the process.
33. Adam White Scoville, *Clear Signatures, Obscure Signs*, 17 Cardozo Arts & Ent. L.J. 345, 349–350 (1999) (emphasis added).
34. A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709, 714 (1995) (emphasis added).
35. *Id.* (emphasis added).
36. *Id.*; *see generally* Scoville, *supra* note 33, at 350; raymond a. kurz, internet and the law: legal fundamentals for the internet user, 156 (1996) (emphasis added).
37. *See* Scoville, *supra* note 33, at 350; Froomkin, *supra* note 34, at 714 (emphasis added).
38. Froomkin, *supra* note 34, at 714.
39. *Id.*; Scoville, *supra* note 33, at 350. Algorithms are almost never kept secret today "because the algorithm's use would be limited to one group of communicants." *Id.*

for the recipient (often called "*enemies, opponents, interlopers, eavesdroppers, and third parties*").[40] It comes as no surprise that third parties want and do read our private emails, follow our transactions online, and obtain our confidential information.[41]

The second answer addresses our three scenarios discussed above.[42] Not only will third parties not be able to read our information, but it is less likely that transmitting parties will be able to blame third parties when problems arise. If keys are keep secret, one party will be able to bind another party to a transaction because it is unlikely that anyone else (who does not have the key) could read, alter, or send the message.

Advances in cryptography allow for two different keys to encrypt and decrypt the message. This is an advance from the *single key system* (symmetric encryption), which allowed for the message to be encrypted and decrypted by the same key.[43]

With current technology *public key system* (asymmetric encryption) algorithms encrypt a message with one key and only allow that message to be decrypted with a different key.[44] The key that encrypts[45] is most likely, but not always the *private key*, and the one that decrypts[46] is most likely, but not always the *public key*.[47] A transacting party can give access to any party they desire. Senders may make this key available through different means including an email message, on their Web site, or in other repositories maintained by third parties.[48] This allows for some transacting parties to give their key to anyone who goes on their Web site and for others to only give their key to known individuals.

For instance, one may want to be able to send messages to a number of people and is only worried about parties being assured the message is from the sender, and has not been changed since it was sent. This party may publish his public key on their Web site because they do not care who is able to decrypt the message.[49] Others, however, may only want one or two parties to be able to decrypt and understand their message. This party may, in private, allow only those chosen individuals to have access to their public key.

---

40. Froomkin, *supra* note 34, at 714 (emphasis added).
41. A common example would be a third party trying to obtain transacting parties' credit card information.
42. *See* discussion *supra* Parts II.A.1–3.
43. Although the significance of this may not be apparent, it soon will be. Two different keys are more secure than one single key in terms of authenticity, integrity, and reliability of the message.
44. Froomkin, *supra* note 34, at 714 (emphasis added).
45. The process of changing the original message into the disguised message. *See* sources cited in *supra* note 36.
46. The process of changing the disguised message back to the original message. *See* sources cited in *supra* note 37.
47. Some parties set up their transactions for the public key holder to encrypt and the private key holder to decrypt. It is determined by the parties' circumstances.
48. Dickie, *supra* note 28, at 36.
49. It is important to note that saying "one does not care who can decrypt the message" does not mean that any person who goes on the private key holder's Web site will be able to read the private key holder's message. It only means that if the holder of a public key receives a message from the private key holder, he will be able to decrypt and read the message. The public key holder still has to be sent a message from the private key holder.

In any case, once an individual obtains the public key they will be able to decrypt and read an encrypted message sent by the private key holder. If the receiving party is able to read the message, meaning it does not appear as "an unintelligible string of characters,"[50] they can be assured that the message came only from the private key holder and that it has not been altered from the time it was sent.[51] Conversely, in some situations the private key holders may be the ones decrypting an encrypted message sent by a public key holder. In this case, depending on how many parties have access to the public key, any number of persons could be sending the private key holder a message. The private key holder may not be able to guarantee who the message is from if he has given his public key to more than one person, but the public key holder is assured that only the private key holder will be able to decrypt and read the message.

To illustrate this interchange, consider the following two examples contrasting single key and public key systems.[52] In a single key system, our sender, Alice, and receiver, Bob, agree on the single key they are going to use to encrypt and decrypt the message. Alice encrypts her message using the key and sends the ciphertext to Bob, who uses the same key to decrypt. Bob can read Alice's original message, but he may not be the only one. This message will only be secure from third parties or eavesdroppers (Eve[53]) if the selection of the single key is done in private. If key selection is done on a public line, like a Web site, then Eve can obtain the key to decrypt the message just as Bob can. More importantly, Eve could encrypt a message, pretending to be Alice, and send it to Bob without him knowing it was not Alice. Single key encryption "is analogous to a combination safe, where both the person putting items into the safe and the person taking them out of the safe must be able to open the combination lock."[54] How secretive and careful the transacting parties are with their keys determines how many people have access to the combination safe.

In a public key system, Alice and Bob have two different but corresponding keys: the public key that Alice will use to encrypt the message and the private key that Bob will use to decrypt it. In this case, Bob can give Alice the public key, in public, without having to worry about Eve learning of it. This is because, even if Eve does learn of it, she will not be able to decrypt the message without the private key, which only Bob has. This scenario using private key encryption "is analogous to a post office box, where anyone can deposit mail once the recipient's specific box number (the public key) is known, although only the box holder with the (private) key can open the box."[55] The only concern about giving the key out in public is that Eve might obtain it and be able to encrypt a message to Bob or deposit mail in his box. If this is a concern, then Bob and Alice have to exchange keys in private. However, it is uncommon for Eve to want to intercept a public key in order to write Bob messages that only he can read.

50. dickie, *supra* note 28, at 36.
51. *See id.*
52. Portions of the examples and the names used are taken from Scoville's article, *supra* note 33, at 350–52. In some parts, the examples have been expanded or retracted to tie in with this article.
53. Hereinafter, "Eve" will be the fictional character that is the eavesdropper.
54. Scoville, *supra* note 33, at 351.
55. *Id.*

The public key system also works the opposite way if the situation requires. Again, Bob can give Alice the public key and keep the private key. In this situation, Bob wants to send an encrypted message to Alice. Alice will be able to decrypt the message with the public key and be assured it is from Bob, the only person who has the private key. In this situation, however, Bob has to make sure that the public key was given in private so that Eve cannot obtain it and decrypt the message. If not, he has to not care if Eve can decrypt and read his message. Parties set up this type of transaction when they are concerned with Alice receiving a message that could only have been sent from Bob. Again, if the parties are worried about third parties reading the messages, they need to exchange their keys in private.

B. Certification Authorities

The question now becomes how electronic signatures provide the trustworthy proof we need. Common sense raises security questions with the public and private key systems. Who is to say that the person you think you are dealing with is not really pretending to be someone else in order to take advantage of the system? Who is protecting Alice and Bob when Eve steals Bob's private key and enters into transactions with Alice? In other words, what type of device will be used to assure that fraud, forgery, and other types of misrepresentation will not be common with electronic transaction?

The answer is Certification Authorities. A Certification Authority "is a [trusted third party] that acts as a repository of public keys and authenticates the relationship between a particular public key and its supplier."[56] Certification Authorities are licensed third parties that are used to certify the holders of public and private keys.[57] They can be used as a means to validate electronic signatures:

> First, the subscriber must generate her own public key–private key pair. The subscriber then visits the [Certification Authorities] and produces proof of identity. Most [Certification Authorities] require an official document with picture identification, such as a driver's license and/or passport. Finally, the [Certification Authorities] will require a demonstration that the subscriber holds the private key corresponding to the public key.[58]

If the process is completed accurately and the subscriber passes the Certification Authority's requirements to verify the association between the subscriber and the public key, the Certification Authority can then issue a certificate.[59] A certificate "is an electronically stored record attesting to the connection between the public key and subscriber."[60] Most basically, it contains the "user's name and public key,"[61] but it can, and most

56. Lupton, *supra* note 27, at 13–14.
57. Randy V. Sabett, *International Harmonization In Electronic Commerce and Electronic Data Interchange: A Proposed First Step Toward Signing On the Digital Dotted Line*, 46 Am. U. L. Rev. 511, 524 (1996).
58. Lupton, *supra* note 27, at 13–14.
59. *Id.*
60. *Id.* at 14.
61. Sabett, *supra* note 57, at 524.

likely does, contain more information.[62] Once the subscriber sees the final certificate and ensures its accuracy, the certificate can be made publicly available.[63] Third parties who want to correspond with the subscriber can do so once the certificate is published. A certificate is officially considered published when it is recorded in a repository.[64] Transacting parties need to be aware that a published certificate is one that has been accepted by the Certification Authorities and the subscriber, and the certificate is, therefore, given a presumption of validity. Consequently, it is important not to transact with a party who does not have a certificate that has been validated.

Certification Authorities have created ways in which to safeguard private keys in case the key gets lost, stolen, or compromised. It is analogous to telling your roommate that you lost the keys to the apartment and are going to have the locks changed. Subscribers (private key holders) should report the key lost or compromised and "should suspend or revoke the certificate corresponding to the key pair immediately."[65] This will give notice to public key holders just as you give notice to your roommate that his or her key is no longer going to work in the apartment lock.

There are usually two ways in which reporting the key lost or compromised provides notice to public key holders that parties other than the original subscriber may be using the private key. Most likely, the repository will contain the status of the private key's certificate: "valid," "suspended," or "revoked."[66] There is also a separate list called the "Certificate Revocation List (CRL), which is a separate database of certificates and their corresponding public keys that have been revoked before their expiration date."[67]

Private key holders are not the only parties who can invalidate a private key. Certification Authorities are contractually permitted to revoke or suspend a certificate when they have reason to believe that the reliability of the certificate has been compromised.[68] They are able to do this even without the private key holder's permission. This will normally happen in two situations. Certification Authorities will revoke or suspend the certificate if they believe that it has been lost or stolen just as the private key holder can, or they will act when they believe that the private key holder made false representation on his application for a certificate.

It is important for a public key user not to correspond with or trust the validity of a private key when its certificate has been placed on a CRL, when it is listed on the repository as "suspended" or "revoked," or when there is another reason to believe that the private key user is not the original subscriber. It is therefore crucial to periodically check the repository list when conducting electronic transactions with another party. It is

62. For instance, the key expiration date, size, and/or signature generation software identifier. *See* Lupton, *supra* note 27, at 13–14.
63. *Id.* The Certification Authority or the subscriber can publish it.
64. *Id.* at 17. "A repository is 'an electronic database of certificates—the equivalent of [an online] digital Yellow Pages' accessible to the general public." *Id.*
65. *Id.* at 13–18.
66. *Id.*
67. *Id.* at 18.
68. *See* Angela Y. Ball, *Are Your Clients Equipped to E-Sign?: Effective Strategies in Negotiating PKI Technology*, E-Com. L. & Strategy (A Division of The New York Law Publishing Co.), Vol. 17; No. 5; at 1, Oct. 2000.

also important for owners of a private key not only to contact the Certification Authorities when they believe their private key has been compromised, but also to personally contact known public key holders. When all parties—the public and private key holders and the Certification Authorities—act responsibly and safely the security and success of electronic signatures will be guaranteed.

IV. Security Services

Now that there is an understanding of how electronic signatures work, one can begin to understand how they will be able to address our current problems[69] with electronic transactions. This is mainly the need to provide trustworthy proof of parties' intent to be bound to their transactions. All signatures, written and electronic, can be used to accomplish certain legal roles or tasks. Five important ones to consider are: (1) authentication, (2) integrity, (3) confidentiality, (4) non-repudiation, and (5) reliability.[70] These roles, when analyzed, can be looked at as security services[71] provided by the signature or ways in which we provide trustworthy proof of the parties' intent of the transaction. Not coincidently, these five security services provided by signatures are the same as the problems previously identified[72] that keep parties from conducting electronic transactions. In most instances, electronic signatures will be able to provide a security service for transacting parties that will limit or eliminate these fears.

A. Authentication

When a digital document is electronically signed one is able to show a connection between the signer and the document. If the signer is to be bound to the document, and therefore the transaction or contract, he must actually be the person entering into the transaction. Certification Authorities provide the information and surety that the person signing with the private key is who he purports to be and that no one other than the holder of the private key has written the message.[73] In other words, this security service "assures the recipient that only the sender could have created the message."[74] Furthermore, it assures him of the "authenticity of the sender's message."[75]

B. Integrity

Integrity means that the contents of the sender's message arrive at the recipient just as they were sent. There is always the possibility that someone could alter the contents

69. See the three scenarios discussed *supra* Parts II.A.1–3, for why transacting parties do not take full advantage of the Internet (authentication, integrity, confidentiality, and reliability).
70. *See* John P. Tomaszewski, *The Pandora's Box of Cyberspace: State Regulation of Digital Signatures and the Dormant Commerce Clause*, 33 Gonz. L. Rev. 417, 419–21 (1997/1998); *see also* Lupton, *supra* note 27, at 15–16; Sabett, *supra* note 57, at 515–17.
71. *See* Sabett, *supra* note 57, at 515.
72. *See supra* note 69 and accompanying text. Note that "reliability" will now be divided into two categories: nonrepudiation and reliability.
73. As long as the key has not been lost, stolen, or compromised.
74. Sabett, *supra* note 57, at 516.
75. *Id.*

of a message after it was sent by the sender and before it arrives at the recipient. If this happens, the sender could be bound to something he did not intend to be bound to.[76] By using private and public keys, there is assurance that the message has not been changed or altered in any way from the time the holder of the private key applied his signature and sent the message. This security service assures that the message is "concealed and secure"[77] and has not been digitally altered from the sender's form.

C. Confidentiality

Confidentiality gives surety that only the sender and receiver can understand the message. Ideally, if an outside party, a third party, intercepted the message, this security service would prevent the intruder from understanding it.[78] Confidentiality can only be provided with electronic signatures and not digital signatures.[79] Encryption technology allows electronic signatures to provide this service. That is, "[e]ncryption mathematically scrambles the communication so that only the sender and recipient can unscramble and understand the original message."[80]

D. Non-Repudiation

A fourth security service provided by electronic signatures is non-repudiation.[81] Just as with written signatures, this service provides that the sender is willing to be bound to the document and, therefore, the transaction or contract.[82] It is logical to say that it is even harder for a signer of an electronic signature to repudiate his or her willingness to be bound to the document.[83] Often with written signatures there are the excuses of fraud, forgery, or mistake. Although these problems may still exist with electronic signatures, the probability is decreased.[84] It is unlikely that "anyone other than the signatory could have signed and sent the digitally signed document. The physical security of [encryption] means that the document must have been signed with the sender's/signatory's private key."[85] Essentially, the security service that nonrepudiation assures is that the sender of the message cannot deny sending the message to the person who received it.

---

76. *See* Tomaszewski, *supra* note 70, at 420.
77. Lupton, *supra* note 27, at 20.
78. Sabett, *supra* note 57, at 515.
79. A digital signature is just a reproduction of the sender's handwritten signature on the screen; it is not a signature that uses encryption technology.
80. *See* Sabett, *supra* note 57, at 515.
81. As Sabett points out in his article, *supra* note 57, there is some confusion with the term non-repudiation. The confusion stems from the fact that "there is no such thing in the legal vernacular as nonrepudiation," combined with the common use of the term "repudiation" in contract law. "Because a party always can try to breach a contract, there really is no legal notion of nonrepudiation. In information security, however, the concept of nonrepudiation is well established." *Id.* at 517.
82. *See* Tomaszewski, *supra* note 70, at 420.
83. *See* Lupton, *supra* note 27, at 25.
84. "It is theoretically possible for another party to discover a private key, even though the key's holder has conscientiously safeguarded it." *Id.* at 26.
85. *Id.* at 25.

E. RELIABILITY

As discussed above,[86] authenticity, integrity, confidentiality, and nonrepudiation are not the only problems that keep Internet users from conducting electronic transactions. Users also have the fear of reliability,[87] which is the fear that electronic transactions will not be considered valid under current law in different countries and jurisdictions. Although transacting parties may begin to personally feel comfortable with electronic transactions because of the other security services provided by electronic signatures, parties are not assured that they are as reliable when compared to written signatures.

Unfortunately, electronic signatures cannot address the reliability problem as they can with the other four problems (authenticity, integrity, confidentiality, and nonrepudiation). In fact, electronic signatures help create the fear of reliability. Parties question whether electronic signatures will be considered valid. Will they just be a presumption of a valid signature? Will they have no legal effect at all? Currently, in most jurisdictions throughout the world, Internet users are just beginning to see how electronic signatures are interpreted in a court of law. As mentioned above, the UCC's Statute of Frauds[88] in the United States requires that certain contracts be in writing and be signed. Under the UCC, "writing" is defined as including "printing, typewriting or any other intentional reduction to tangible form."[89] While it seems clear from court rulings that the writing requirement will be satisfied by electronic transmission, it is not as clear if the signature requirements will be.[90] "Signed" is defined under the UCC as including "any symbol executed or adopted by a party with present intention to authenticate a writing."[91] The Official Comment to UCC §1–201(39) leads one to believe that the drafters intended a far-reaching definition of "signed":

> The inclusion of authentication in the definition of 'signed' is to make clear that as the term is used in this Act a complete signature is not necessary. Authentication may be printed, stamped or written; it may be by initials or by thumbprint. It may be on any part of the document and in appropriate cases may be found in a billhead or letterhead. No catalog of possible authentications can be complete and the court must use common sense and commercial experience in passing upon these matters. The question always is whether the symbol was executed or adopted by the party with present intention to authenticate the writing.[92]

One can make a strong argument that electronic signatures should be considered valid where the law requires. However, parties are unwilling to use electronic transactions on the assumption that a court of law is going to agree with that argument. Transacting parties want reliable proof before they enter into a transaction that it is going to be considered valid proof of both parties' intent. Furthermore, a few court rulings that do consider electronic signatures valid will not help the problem. Parties recognize that states and countries do not necessarily follow each other's rulings. Transacting parties need a law that governs the validity of their electronic transactions.

86. *See supra* Parts IV.A–D.
87. *See supra* Part IV.E.
88. *See supra* note 19 and accompanying text.
89. U.C.C. §1–201(46) (2000).
90. *See* JOHNSTON, *supra* note 20, at 192.
91. U.C.C. §1–201(39) (1997).
92. *Id.* at Official Comment to (39).

V. What an Ideal Electronic Signature Law Encompasses

A. Purpose of a Global Law

When considering the purpose of a model law regarding electronic signatures and the provisions it should contain, it is important to concentrate on why the law is needed. Basically, the need is created because transacting parties want a way to provide "trustworthy proof" of parties' intent to be bound to their electronic transactions—the same type of "trustworthy proof" that is currently provided by handwritten signatures on written documents.[93] From this central need, the purpose of a model law can be specifically stated as a need for authenticating and legally recognizing electronic transactions between parties through electronic signatures. Furthermore, the purpose of a model law should also be to attain international compatibility between all countries in the world.

B. Allow for the Qualities and Attributes of Written Signatures to be Adopted in Electronic Ones

As discussed throughout this article, electronic signatures will allow parties to show their intent to be bound to transactions in cyberspace, which will in turn create confidence in the validity of electronic transactions and encourage more parties to use cyberspace as a tool, which will lower transaction costs and produce economic growth. Parties "need to be sure that when they're using an electronic signature, it's as secure as putting pen to paper."[94] Therefore, electronic signatures need to encompass the same qualities and attributes as written signatures. In Richard Allan Horning's article, *Legal Recognition of Digital Signatures: A Global Status Report*, he describes seven reasons why the "signed writing" was developed:

> First, there is the evidentiary value of having a permanent embodiment of the transaction. A writing produces this. Second, we can see the value of the ceremony, which was a major concept in 1677.[95] We lawyers all remember the concept of 'livery of seisin' in connection with real estate transactions from our course in Real Property—the crumbling of some soil in the presence of the transferee as a part of the ceremony where Blackacre changed hands. Third, the affixing of a signature as indicating approval. 'By signing this document I acknowledge it as an agreement I stand behind.' Fourth, clarity. Clarity arises from the very act of forcing the contracting parties to express their intent in a written document. Fifth, finality. Finality is the notion that the signed document embodies the final agreement of the parties superseding all the unsigned drafts. Sixth, the deterrence of doubtful transactions. This was a primary reason in 1677—if one reads the case law—to have a writing requirement. Finally, written documents provide an ease of negotiation. This allows the creation of what have become known as 'negotiable instruments.'[96]

Horning's list recognizes important qualities and attributes that written signatures hold today. In order for electronic signatures to become universally accepted, similar qualities and attributes need to be recognized in electronic signatures in the same way

93. Meaning handwritten and typed documents; tangible documents.
94. *Supra* note 25.
95. The conception date of the Statute of Frauds.
96. Horning, *supra* note 16, at 193–194.

they have become recognized in written signatures. An ideal international model law should provide room for similar qualities and attributes to be found in electronic signatures as are found in written ones. This ideal is easily stated but is a much harder realization. Lawmakers cannot just write law and give electronic signatures these qualities and attributes. Qualities and attributes are realized over time by society as a whole.

Ideally, society's acceptance will happen almost simultaneously through two channels: (1) Internet users (consumers, businesspersons, and governments) and (2) lawmakers. Both channels will feed off each other in order for the qualities and attributes of written signatures to be adopted in electronic ones. Internet users will continue to recognize the immense benefits that the Internet has to offer and will, therefore, increase the amount of electronic transactions they conduct. As governments and courts recognize the increasing use of electronic transactions, they will acknowledge the need for laws governing electronic transactions and electronic signatures. As a result, legislators will write new laws and courts will interpret existing laws that legally acknowledge the electronic transaction process and electronic signatures. Consequently, the Internet users will gain confidence in electronic transactions and continue to increase their use.

As these channels work off each other throughout the next couple of years, electronic signatures will begin to acquire the qualities and attributes that written signatures currently hold. This will happen as both lawmakers give legal significance to the electronic transaction process, and Internet users become more familiar with electronic transactions. For Internet users, this includes not only the process of conducting transactions electronically, but also an understanding of how their electronic actions are interpreted in a court of law.

This concept may be hard to grasp at first until you consider the evolution of handwritten signatures. The qualities and attributes associated with handwritten signatures did not appear overnight. Like electronic signatures, there was a need, created by society, to have "formal recognition between contracting parties of the making of and existence of their contractual relationship."[97] This need developed over time and governments reacted to this need by creating law. But even in situations where the law did not govern written contracts and signatures, the process and value of signing your name or symbol to a document became recognized. This was a result of society becoming familiar with the process of signing their name and with an understanding of the legal significance of doing so. Society realized that by signing a document they were in turn accepting or indicating approval to what that piece of paper purported to say or accomplish. The same course of development that happened with written signatures can and most likely will happen with electronic signatures when governments and Internet users begin to work off each other.

C. Lawmakers' Considerations for an Electronic Signature Law

In view of the fact that Internet users are in actuality increasing the number of transactions done electronically, the feeding effect discussed above[98] has already begun.

97. *Id.* at 192.
98. *See* discussion *infra* Part V.B.

It is now time for lawmakers to write or interpret law considering electronic signatures. Even though lawmakers cannot give electronic signatures the qualities and attributes of written signatures, they can write laws that place the two signatures on the same level, legally. There are five general areas that lawmakers should consider when legislating electronic signatures: evidentiary value, allowance for changes in technology, intent of parties, preference between signature types, and international compatibility.

1. Evidentiary Value

Lawmakers should address the evidentiary value of an electronic signature. This means that electronic signatures should not necessarily have a presumption of validity as written signatures do.[99] Lawmakers should, however, be careful to make sure that electronic signatures are not denied legal effect just because they are electronic. When lawmakers accept electronic signatures' validity, society will begin to demand them in transacting in order to have a "permanent embodiment of the transaction."[100] The more society demands electronic signatures in electronic transactions, the more common and accepted they will become.

From this, it is also easy to see how electronic signatures will be used to "indicate approval,"[101] and create "finality"[102] and "clarity"[103] in transactions, just as written signatures can. As society realizes that electronic signatures have much the same legal and social effect as written signatures, they will demand them in order to express their intent, indicate their approval, and finalize their transactions.

2. Avoid Preferences Between Signatures

Any legislation enacted governing electronic signatures should avoid interfering with the validity of traditionally valid written signatures. Legislation should not favor one form of contracting over another. This means that when writing new laws concerning electronic signatures, they should not be given preferential or lesser significance than written signatures. This may seem like an obvious criterion, but it is important for legislators to keep this in mind when writing new law. They may inadvertently make it more or less beneficial for parties to use electronic signatures.

In either case, there may be negative consequences. If electronic signatures are found to be less favored in the law, parties will not want to use them. They will fear that their transactions will not be considered valid. On the other hand, if they are favored over written signatures, parties with power may require that electronic signatures be used. This has the potential to affect parties who are not yet comfortable with the technology but are forced to use it. In turn, parties may be taken advantage of.

---

99. Note, however, that this could eventually happen in the future.
100. *See* Horning, *supra* note 16, at 193–94.
101. *See infra* Part V.B.
102. *Id.*
103. *Id.*

3. *Avoid Interfering with the Intent of Contracts*

Electronic signatures also need to "avoid interfering with the validity of electronic authentication procedures agreed to by contract."[104] This is extremely important because there should be legislation that does not harm those who do not yet feel comfortable with conducting electronic transactions. Parties should be allowed to contract around any legislation if they feel it would be better for their particular transaction. For example, this would include clauses in contracts stating that any form of electronic data interchange will not be considered binding to the parties, and that written signatures are required to finalize all agreements.

4. *Technology-Neutral*

Electronic signature legislation should be technology-neutral. Basically, this means that laws should not favor one form of electronic signature technology over another. This is imperative for a number of reasons. First, as we have already seen in the last decade, technology can advance right before our eyes. Therefore, it is important that any legislation does not impede further technology by limiting it. One should be able to interpret the legislation broadly so as to include technological advances that most likely will come in the future. The explanatory memorandum to Australia's Electronic Transactions Bill of 1999 follows this theory by explaining, "by not endorsing particular electronic signature technologies, the Bill does not need to be revised to take account of technological changes."[105]

Second, this is also important for competition in the marketplace. If the legislation is technology-neutral it will not favor one form of electronic signature, Certification Authorities, and so forth. This in itself will encourage advances in technology and allow for more companies to become players in the market and decrease prices.

5. *International Compatibility*

The positive and encouraging news is that electronic signatures are emerging quickly and most international countries are responding by developing laws and legislation to govern the new technologies. The negative side is that there appears to be less concern on developing uniform international laws and legislations to govern the same advantageous technologies. This is perhaps the most important factor for lawmakers to consider when legislating electronic signatures.

The United States can be used as an example of problems that will arise if countries do not adopt a uniform or compatible international body of law governing electronic signatures. In the United States, most individual state legislatures have passed or addressed issues concerning electronic signatures but "there is no national standard," as each state has its own set of rules governing electronic signatures. The differences range from what kinds of electronic signatures they may use to what circumstances they may use them in, to whom in particular may use them. Some states provide that any type of electronic signature is valid. Others require that some minimal form of security is required (such as tying the electronic signature to the signer or being able to ascertain that the message

104. Scoville, *supra* note 33, at 349.
105. Kanthan, *supra* note 6, at 26.

has not been altered). Still other states validate only digital signatures, thought to be the most secure and requiring the use of encryption.

For instance, while Utah and Washington "permit the use of [electronic] signatures for almost all public and private forms of communication, Alabama's state government only recognizes [electronic] signatures when filing tax returns and other documents with the Department of Revenue."[106] In Hawaii, you can use electronic signatures, "but only to file electronically court documents."[107] Conversely, some states have gone in the other direction and have enacted far-reaching electronic signature legislation, including Georgia, West Virginia, Iowa, Illinois, Wisconsin, Kansas, and others.[108]

The problems begin to become apparent. What is going to happen when someone in Illinois with far-reaching use of electronic signatures is dealing with someone in Hawaii who has limited use of electronic signatures? Will they be able to use electronic signatures at all, and whose law will govern?[109] Although federal legislation could develop laws that govern how states should govern the difference, it is probably wiser to just develop a uniform law. This is, in fact, what the Federal Government of the United States has done.

On June 30, 2000, President Clinton signed the Electronic Signatures in Global and National Commerce Act (E-Sign),[110] which became effective on October 1, 2000.[111] E-Sign grants electronic signatures and documents equivalent legal status with traditional handwritten signatures. It is technology-neutral so that the parties entering into electronic contracts can choose the system they want to use to validate an online agreement. The U.S. Congress wrote the federal statute to address the problems created by having, in some cases, extremely different state legislation governing electronic signatures.[112]

If one considers the varying legislation that has been passed in the individual states of the United States, it becomes apparent why there is a need for uniformity. Currently, countries have immensely dissimilar legal systems, which obviously operate differently. The need for uniformity grows even more when we consider the international setting. The need for federal legislation in the United States is similar to the need for an international model around the world. A harmonized law that is universally accepted is a difficult task to accomplish when one considers the immense differences in attitudes, cultures, economies, legal systems, and technology.[113] Enactment of an international model law is an important task that needs to be completed before technology gets too far ahead

106. Kalama M. Lui-Kwan, *Business Law: 1. Electronic Commerce: a) Digital Signatures: Recent Developments in Digital Signature Legislation and Electronic Commerce*, 14 BERKELEY TECH. L.J. 463, 472–73 (1999).

107. *Id.* at 473.

108. *See id.* at 473–74.

109. Note that these problems are very similar to those addressed by the Uniform Commercial Code.

110. Electronic Signatures in Global and National Commerce Act (E-Sign), Pub. L. No. 106–229, 114 Stat. 464 (2000) [hereinafter E-Sign].

111. *Id.*

112. E-Sign will be discussed in more detail later in the article.

113. *See* A. Brooke Overby, *UNCITRAL Model Law on Electronic Commerce: Will Cyberlaw Be Uniform? An Introduction to the UNCITRAL Model Law on Electronic Commerce*, 7 TUL. J. INT'L & COMP. L. 219 (1999).

of the law; "only through such harmonization can the uniformity of law that is so crucial to support efficient and fair commercial transactions be advanced."[114]

VI. What Has Been Accomplished So Far?

Internationally, numerous groups, governments, and other bodies have recognized these needs and have been developing legislation and regulations for electronic signatures and Certification Authorities.[115] When evaluating these current laws, one should consider and compare them to the standards set out above:[116] evidentiary value, allowance for changes in technology, intent in parties' contracts, preference between signature types, and international compatibility.

A. UNCITRAL

The United Nations Commission on International Trade Law (UNCITRAL), a body of the United Nations, is one such body that has been developing legislation.[117] For a number of years, this body "has been promoting a Model Law on Electronic Commerce and Draft Uniform Rules on Electronic Signatures."[118] In summary, UNCITRAL applies where electronic signatures are "used in the context of commercial activities."[119] The term "commercial" is intended to be interpreted broadly so as to include as many transactions as possible.[120] The drafters are careful to mention in a footnote that the "[l]aw does not override any rule of law intended for the protection of consumers."[121] It also allows for

114. *Id.* at 219–20.

115. For a current summary of electronic signature legislation of specific countries, see McBride Baker & Coles' Summary of Electronic Commerce and Digital Signature Legislation, *available at* http://www.mbc.com/ecommerce.html. Other bodies currently developing legislation or trying to enact legislation that are not discussed in this article include (but are not limited to): the World Trade Organization (WTO), the International Chamber of Commerce (ICC), International Secure Electronic Transaction Organization, International Telecommunication Union (ITU), United Nations (UN), Organization for Economic Co-operation and Development (OECD), and National Conference of Commissioners on Uniform State Laws (NCCUSL).

116. *See supra* Parts V.C.1–5.

117. UNCITRAL Model Law on Electronic Commerce (1996) (amended 1998), *available at* http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm [hereinafter UNCITRAL]. Since February 1997, the UNCITRAL Working Group on Electronic Commerce has been addressing the task of drafting model international electronic and digital signature legislation. The new Model Law and a Guide to Enactment will be presented to the Commission in Vienna in June–July 2001. This Model Law is virtually identical to the Uniform Rules drafted from March 2000, and is intended to be a companion to the 1996 Model Law on Electronic Commerce.

118. Horning, *supra* note 16, at 198.

119. UNCITRAL, *supra* note 117, art. 1.

120. "The term 'commercial' should be given a wide interpretation so as to cover matter arising from all relationships of a commercial nature, whether contractual or not." *Id.*

121. UNCITRAL, *supra* note 117, art. 1.

individual states to put limits on how broadly the term "commercial" may be interpreted or what it may include.[122] This is important in two respects.

First, the law seems to be technology-neutral when it says "any kind of information in the form of a date message."[123] The Model Law does not make specific references to encryption, cryptography, or Certification Authorities but it adopts a "limited framework" for regulating e-commerce.[124] This means that the Model Law is not a "comprehensive, 'code-like' articulation of the rules and regulations for electronic information transmission, nor intended to govern every aspect of e-commerce."[125] It is clearly intended to be technology-neutral. Second, it has the ability to avoid interfering with parties' intent of contracts. This is because a state may narrow the statute to exclude transactions where the parties intended not to have electronic signatures be considered valid.

Furthermore, the Model Law does not take a stance on "evidentiary presumptions or liability limits, involving the use of electronic signatures."[126] The Model Law states, "[i]nformation shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message."[127] This is to say, the Model Law does not have a presumption in favor of or against electronic signatures. Additionally, Article 9 states,

> [i]n any legal proceeding, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence: (a) on the sole grounds that it is a data message or (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.[128]

This provision in the Model Law is extremely important because parties will no longer have a fear that their electronic data transactions will not be able to be offered as proof of the transaction in a court of law.

The Model Law goes further to help ensure that an electronic document will not be denied legal effect just because it is electronic. In Article 6, the Model Law states that any legal requirement that information be in "writing" will be "met by a data message if the information contained therein is accessible so as to be usable for subsequent reference."[129] Article 7 allows for electronic signatures to be considered valid signatures where the law

122. In UNCITRAL, Article 1, the Drafters suggest the following to be inserted into individual State law that might wish to extend the applicability of the Law: "This Law applies to any kind of information in the form of a date message, except in the following situations: . . . ." *Id.*

123. *Id.* and accompanying text.

124. *See* Overby, *supra* note 113, at 222.

125. *Id.*

126. Scoville, *supra* note 33, at 385–86.

127. UNCITRAL, *supra* note 117, art. 5. Article 5 was amended in June 1998. It previously read: "Information shall not be denied legal effect, validity or enforce-ability solely on the grounds that it is in the form of a data message."

128. UNCITRAL, *supra* note 117, art. 9.

129. *Id.* art. 6.

requires signatures if certain conditions are met, to wit:

> Where the law requires a signature of a person, that requirement is met in relation to a data message if (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.[130]

This signature provision is written in such a way that it effectively avoids having a preference between written and electronic signatures.

UNCITRAL has been working on a more detailed set of rules to specifically govern electronic signatures.[131] This Draft takes positive steps towards accepting the validity of electronic signatures. In this Draft, there are "rebuttable presumptions that: (1) the document was signed; (2) the signature is that of the purported signer; (3) the document's integrity is intact; and (4) the purported signer is still liable for unauthorized signatures if he failed to take reasonable care to avoid such unauthorized use."[132]

UNCITRAL's Model Law is a good example of legislating electronic signatures in a way that will place electronic communications and transactions on par legally with traditional paper-based ones. It effectively addresses the issues of evidentiary value, technology changes, intent of contracts, and preferences between written and electronic signatures. What UNCITRAL does not address is international aspects of electronic signatures. This is something that legislatures should consider for future drafts or changes.

B. EU

The European Parliament has taken positive steps towards adopting successful regulation regarding electronic signatures. In December 1999, the European Parliament and the Council adopted *Directive 1999/93 on a Community Framework for Electronic Signatures.*[133] The Directive is intended to apply generally to all communications. The purpose and scope of the Directive is clearly stated therein: "to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market."[134]

---

130. *Id.* art. 7.
131. *See* Draft Uniform Rules on Electronic Signatures, U.N. Commission on International Trade Law, Working Group on Electronic Commerce, 34th Sess., U.N. Doc. A/CN.9/WG.IV/WP.79 (1998), *available at* http://www.un.or.at/uncitral/English/sessions/wgec/wp-79.htm [hereinafter UNCITRAL Draft Uniform Rules].
132. Scoville, *supra* note 33, at 397 (quoting UNCITRAL Draft Uniform Rules, *supra* note 131, art. 7).
133. Council Directive 1999/93/EC on a Community Framework for Electronic Signatures, 2000 O.J. (L 13) 12 [hereinafter Directive]. The law is supposed to be complied with by July 19, 2001. *See id.* art. 13.
134. *Id.* art. 1. "It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents." *Id.*

The intended consequence of the EU Directive was to "make electronic signatures as easily employable as handwritten ones."[135] The Directive successfully outlines a legal framework for not only electronic signatures but also for Certification Authorities. It is not designed to regulate everything in detail but defines the requirements for electronic signatures certificates and Certification Authorities in order to ensure minimum levels of security and all their free movement throughout the Internal Market. For this reason, the Directive appears to be relatively short and noncomplex. The key elements of the Directive are legal recognition, free circulation, liability, a technology-neutral framework, scope, international dimension and legal effect.

When reading the Directive's definition of an electronic signature, one can assume the Act is intended to be technology-neutral. An 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."[136] This clearly does not favor a certain type of signature technology over another and seems to be a definition that allows for technological advances. The Directive does, however, add another definition of electronic signature, calling it an "advanced electronic signature."[137] This is a signature that 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 means 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.[138]

Although it is unclear why there is a need for two definitions, one can see that the "advanced electronic signature" is more secure and reliable than the ordinary "electronic signature." It is probably practical to have the two definitions. Not only does it make the law more technology-neutral, but it also seems to allow parties to contract with different signatures in mind. Some parties may only want a little security and others may require more. The Directive will allow them to insert the appropriate language in their contract and have statutory definitions already prescribed.

The Directive also gives great evidentiary value to electronic signatures. Article 5 states that Member States shall ensure that electronic signatures, which are "based on a qualified certificate"[139] and which are secure: "(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings."[140]

The law not only clarifies when the signatures are admissible, but also states when they cannot be denied legal effect. In Article 5, Section 2, the Directive states that Member States cannot deny the legal effectiveness and admissibility of an electronic signature "as evidence in legal proceedings solely on the grounds that it is: in electronic form, or

135. Parmentier, *supra* note 23, at 252.
136. *See* Directive, *supra* note 133, art. 2(1).
137. *Id.* art. 2(2).
138. *Id.* arts. 2(2)(a–d).
139. *Id.* art. 5(1).
140. *Id.* arts. 5(1)(a–b).

not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature-creation device."[141] Overall, the law covers all bases in assuring that an electronic signature will be given appropriate evidentiary value.

Even though the law does not directly address the issue of preferences between electronic and written signatures, it can be presumed that there is not intended to be one. When reading Article 5 on the legal effects of electronic signatures, it appears that they are as valid, but not more valid, than written signatures. This is important. As discussed above,[142] lawmakers want to be sure not to inadvertently favor electronic signatures over handwritten ones. Lawmakers need to realize that not all parties will want to utilize electronic signatures, immediately or at all, and they should not be at a disadvantage because of their preference.

Unlike UNCITRAL, the Directive does successfully address the aspects of international compatibility. It not only tells Member States when to consider third country electronic signatures valid, but it also directs the Commission to make proposals and changes to the Directive as needed to keep up with international compatibility. Article 7, Section 1, states that "Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recogni[z]ed as legally equivalent to certificates issued by a certification-service-provider established within the Community,"[143] if certain requirements are met. At a minimum, it only makes third country parties fulfill the requirements that are set out in the Directive for Member States parties to fulfill.[144]

The most remarkable aspect of the Directive is its encouragement toward the Commission to stay on top of the law and keep the EU compatible with other third countries.[145] Article 7 allows the Commission to make proposals and change the law as appropriate "[i]n order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries."[146] The Directive clearly wants the EU to stay compatible so as not to fall behind in the digital age. Overall, the Directive addresses all the aspects discussed above, and for the most part has addressed them successfully. The only question now is whether all individual Member States will adopt the Directive by July 2001, as required.[147]

141. *Id.* art. 5(2).
142. *See supra* Part V.C.
143. Directive, *supra* note 133, art. 7(1).
144. *Id.* arts. 7(1)(a–c). "(a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or (b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or (c) the certificate or the certification-service-provider is recogni[z]ed under a bilateral or multilateral agreement between the Community and third countries or international organi[z]ations." *Id.*
145. *See* Directive, *supra* note 133, art. 7(3).
146. *Id.* art. 7(2).
147. *See supra* note 134 and accompanying text.

C. E-SIGN

The Electronic Signatures in Global and National Commerce Act (E-Sign)[148] is another example of a government moving in a positive direction with electronic signatures. E-Sign became effective in the United States in October 2000.[149] This law promotes electronic signatures and e-commerce by verifying[150] that electronic signatures will not be denied legal effect. Generally, E-Sign applies to contracts, agreements, or records entered into or provided in, or affecting, interstate or foreign commerce.[151]

Like other regulations discussed thus far, E-Sign also effectively gives electronic signatures evidentiary value. The Act states, "(1) a signature . . . may not be denied legal effect, validity, or enforceability solely because it is in electronic form and (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation."[152] This provision plainly states that electronic signatures will not be denied validity just because they are in electronic form. In doing so, however, it is careful not to favor electronic signatures over written signatures.

A unique provision in E-Sign, which is not as clearly stated in the other two acts, is the Preservation of Rights and Obligations Section. This section effectively avoids interfering with parties' intent of contracts. The provision makes sure that the Act does not "require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party."[153] In so stating, the Act assures that parties will not be forced to use electronic signatures when they do not want to, unless they have agreed to do so in a contract to which they are a party.

The only problems that may arise with this section come in terms of "form contracts."[154] Consumers or other unpowerful and unsophisticated parties may be forced to sign form contracts that require electronic signatures. In this instance, one could argue that they were party to the contract and should be held to the signatures requirement. When interpreting this provision, judges should consider if the parties were on equal negotiating ground when each signed the contract. It does not seem fair to subject an unsophisticated party to technological advances that are above their knowledge and means.

E-Sign also appears to be a technology-neutral law. One of the ways it directly appears to be technology-neutral is the fact that it preempts state law to the extent that state law is not technology-neutral.[155] Another proof of its neutrality can be found in E-Sign's definition of electronic signature: "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or

148. *See supra* note 110.
149. *Id.*
150. It is questionable to some whether this verification was necessary because many believe that the current law defining signatures already encompassed electronic signatures.
151. *See* E-Sign, *supra* note 110, §101.
152. *Id.* §§101(a)(1–2).
153. *Id.* §101(b)(2).
154. Meaning consumer contracts where only the names and quantities are filled in on the forms, but all the terms stay the same.
155. *See* E-Sign, *supra* note 111, §102(a)(2A)(ii).

adopted by a person with the intent to sign the record."[156] As one can undoubtedly see, this definition is not favoring or encouraging one form of technology over another. In fact, this definition, unlike other definitions of the term electronic signature, includes "sound." This clearly seems to be allowing for technological advances. The question may then become: What is not an electronic signature? The Act provides,

> A workable e-signature must: (1) Inform signers what they are doing as they approve documents. It must alert signer they are about to sign important documents, and if they don't wish to do that they must stop; (2) Keep a good record or transcript of the signing event. That's so courts later can determine who signers were, which documents they thought they were signing, and what they intended their signatures to mean (accepting a legal obligation or just acknowledging having seen, though not necessarily approved, the document; [and] (3) Be applied to a document in such a way that the entire document—including all signature evidence and the audit trail—can be given to and stored by both the signer and the receiving party (such as a lender).[157]

Overall, this is a broad, yet specific definition of what electronic signatures are. Users will clearly be able to know what is and what is not an electronic signature.

Fortunately, like the EU's Directive, E-Sign successfully addresses international compatibility of electronic signatures. E-sign encourages and requires the Secretary of Commerce to "promote the acceptance and use, on an international basis, of electronic signatures in accordance with the principles"[158] of the Act. E-Sign states that the Secretary of Commerce should try to eliminate all obstacles holding back electronic signatures "for the purpose of facilitating the development of interstate and foreign commerce."[159] This is a good example of a nation trying to encourage the use of electronic signatures internationally.

VII. Conclusion

Any time governments and other bodies try to create a uniform legal system there will be problems and hardships. This is especially true when no legal rules and regulations existed before the attempt to uniform, as with electronic signatures. It is important, however, for countries around the world to overcome this hardship. Transacting parties' fear of authenticity, integrity, confidentiality, non-repudiation, and reliability are stopping them from utilizing advantageous technology that is available to them. There is no way for parties to show their intent to be bound to their transactions. Fortunately, the technology behind electronic signatures is quickly advancing and is able to cure many of these fears. Nevertheless, no matter how advanced electronic signatures become they will not be able to cure transacting parties' fears of reliability. Lawmakers, legislators, and governments around the world are the only ones who can cure this fear. They have the ability to put electronic signatures on the same level legally as written ones. Once this

156. *Id.* §106(5).
157. Benjamin Wright, *Laws Guide Uniformity For E-Signatures; Electronic Signatures in Global and National Commerce Act*, CREDIT UNION EXECUTIVE, Nov. 1, 2000, No. 6, Vol. 40, at 17.
158. E-Sign, *supra* note 110, §301(a)(1).
159. *Id.*

happens the fear of reliability will be reduced and transacting parties will become more comfortable with conducting electronic transactions.

Electronic signature technology has the potential to influence the future of e-commerce if appropriate internationally accepted legislation is adopted. "Given the global nature of electronic commerce, it is important for as many countries as possible to approach these new legal issues jointly from the beginning and thus avoid having to counter potentially disparate national initiatives."[160] It is obvious that without international legal recognition of electronic signatures and providing for the legal and institutional infrastructure needed for ensuring security of electronic transactions, electronic commerce will not reach its potential.

Recognizing that a single international model law is most likely impracticable, individual nations must individually strive for international compatibility of electronic signatures. This means that the laws of individual nations should be sure to recognize and account for international e-commerce through electronic signatures. They should try to make it as easy as possible for e-commerce to succeed across international lines.

160. Parmentier, *supra* note 23, at 253.