UIC John Marshall Journal of Information Technology & Privacy Law

Volume 17
Issue 3 *Journal of Computer & Information Law - Spring 1999*

Article 2

Spring 1999

Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce, 17 J. Marshall J. Computer & Info. L. 723 (1999)

Thomas J. Smedinghoff

Ruth Hill Bro

ARTICLES

MOVING WITH CHANGE: ELECTRONIC SIGNATURE LEGISLATION AS A VEHICLE FOR ADVANCING E-COMMERCE

by THOMAS J. SMEDINGHOFF† & RUTH HILL BRO††

† Thomas J. Smedinghoff is a partner with the Chicago law firm of McBride Baker & Coles (www.mbc.com), where he leads the firm's Information Technology & Electronic Commerce ("ITEC") Law Department. He is chair of the Illinois Commission on Electronic Commerce and Crime and author of the recently enacted Illinois Electronic Commerce Security Act 5 ILL. COMP. STAT. 175 (effective July 1, 1999). He is also chair of the Electronic Commerce Division of the American Bar Association ("A.B.A.") Section of Science & Technology, and chair-elect of the A.B.A. Section of Science & Technology. He is a member of the U.S. Delegation to the United Nations Commission on International Trade Law ("UNCITRAL"), through which he participates in its Working Group on Electronic Commerce that is drafting international electronic and digital signature legislation, and is the editor and primary author of the book on electronic commerce titled: ONLINE LAW (1996). He received a bachelor of arts degree from Knox College and a juris doctor degree from the University of Michigan Law School.

†† Ruth Hill Bro is an associate with McBride Baker & Coles and a member of its ITEC Law Department. She has co-authored several books and articles on information technology and e-commerce law topics, including ONLINE LAW (1996), INTERNET IN THE WORKPLACE: MANAGING ORGANIZATIONAL ACCESS (1997), and *Organizing Through Cyberspace: Electronic Communications and the National Labor Relations Act*, EMPLOYEE RELATIONS L.J. 341 (1998), and frequently speaks about Internet, electronic mail, e-commerce, and information technology law issues. She received a bachelor of arts degree from Northwestern University and a juris doctor degree from the University of Chicago Law School.

I. INTRODUCTION

As Robert F. Kennedy once observed, "Just because we cannot see clearly the end of the road, that is no reason for not setting out on the essential journey. On the contrary, great change predominates the world, and unless we move with change we will become its victims."[1]

The business world has taken this to heart when it has come to the Internet. Companies have ventured onto the Information Superhighway in increasing numbers to "reduce distribution and marketing costs . . . eliminate the middleman . . . increase efficiency, promote impulse transactions and streamline distribution to far-flung locales" as well as to "connect directly with consumers at home . . . streamline operations and

1. THE QUOTABLE LAWYER § 18.19, at 38 (David S. Sharager and Elizabeth Frost eds., 1986) (citing Robert F. Kennedy's farewell statement, Warsaw, Poland, which was reported in the N.Y. Times, July 2, 1964).

internal transactions, and increase business-to-business sales."[2] The value of U.S.-based e-commerce transactions was estimated to be $43 billion in 1998, and is projected to grow to $1.3 trillion by 2003, over nine percent of total U.S. business sales.[3] More importantly, electronic commerce ("e-commerce") stands on the threshold of broad global acceptance. According to projections by one research firm, worldwide e-commerce sales will reach as high as $3.2 trillion in 2003, representing nearly five percent of all global sales.[4] Significantly, business-to-business transactions have been the most common form of e-commerce, accounting for approximately eighty percent of online transactions.[5]

Likewise, governments around the world have enthusiastically embraced e-commerce as a positive development that should be encouraged. For example, numerous governments have announced that fostering e-commerce is a major public policy objective.[6] Indeed, governments themselves have benefited from the e-commerce revolution by launching their own Web sites to better communicate with and serve constituents while reducing transaction costs.[7]

State upon state, and country upon country, have noted this movement online and responded by proposing, and in many cases enacting, e-commerce legislation and regulations on a wide variety of topics: taxation of e-commerce transactions, jurisdiction over online transactions,

---

2. Margaret Littman, *Cyberspace Race: Online Sales Projected to Reach $368 billion in 2002*, CRAIN'S CHI. BUS., Nov. 30, 1998, at SR1.

3. Forrester Research, Inc., *U.S. On-Line Business Trade Will Soar to $1.3 Trillion by 2003, according to Forrester Research* (visited Dec. 17, 1998) <www.forrester.com/Press/Releases/Standard/0,1184,121,00.html>.

4. Forrester Research, Inc., *Forrester Estimating Worldwide Internet Commerce Will Reach as High as $3.2 Trillion in 2003* (visited Nov. 5, 1998) <http://www.forrester.com/er/press/releases/standard/0,1358,144,ff.html>.

5. Anne Moore, *A Medium That's Not for Everyone*, CRAIN'S CHI. BUS., Nov. 30, 1998, at SR5.

6. *See, e.g., A Framework for Global Electronic Commerce* (July 1, 1997) <http://www.ecommerce.gov/framewrk.htm> (noting that the global information infrastructure "has the potential to revolutionize commerce . . . by dramatically lowering transaction costs and facilitating new types of commercial transactions" and stating that "[t]o encourage electronic commerce, the U.S. government should support the development of both a domestic and global uniform commercial legal framework that recognizes, facilitates, and enforces electronic transactions worldwide"); European Commission, *Proposal for European Parliament and Council Directive on a Common Framework for Electronic Signatures*, (May 13, 1998) <http://www.ispo.cec.be/eif/policy/com98297.htm> (stating that "[e]lectronic commerce presents the European Union with an excellent opportunity to advance its economic integration").

7. *See, e.g.*, U.S. General Services Administration, *Access Certificates for Electronic Commerce* (visited April 9, 1999) <http://www.gsa.gov/aces>. This program is designed to facilitate public access to the services offered by government agencies through use of information technologies, including online access to computers for purposes of reviewing, retrieving, providing, and exchanging information. *Id.*

data protection and data privacy, confidentiality of e-commerce transactions (including export controls of encryption products), unsolicited commercial e-mail (spam), information security, and the enforceability of e-commerce transactions. In some cases, the legislation has been intended to promote and facilitate what is seen as a desirable public policy. In other cases, however, it has been intended to control it.

The enforceability of e-commerce transactions is the most basic and fundamental issue to be addressed by e-commerce legislation. Moreover, it is the subject that has seen the most activity, generally in the form of electronic signature legislation.

Stimulated by the development of the American Bar Association Digital Signature Guidelines,[8] electronic signature legislation began with the Utah Digital Signature Act,[9] which was enacted in 1995 and focused solely on issues raised by cryptography-based digital signatures. Soon thereafter, legislation was introduced in several other states. Yet, the second state to introduce such legislation, California, quickly changed its direction by adopting a very minimalist and technology-neutral approach limited to transactions with state government agencies.[10] Subsequent legislation rapidly migrated from technology-specific statutes focused on digital signatures to technology-neutral statutes that focused generally on all types of electronic signatures.

At last count, forty-nine states, the U.S. Federal Government, and the governments of over fifteen countries have enacted or are currently considering some form of electronic signature legislation.[11] In the U.S. alone, fifty-seven new electronic signature bills were introduced in the state legislatures during the first two months of 1999.[12] In addition, the National Conference of Commissioners on Uniform State Laws ("NCCUSL") is completing a project to develop a Uniform Electronic Transactions Act ("UETA") in the U.S.;[13] the European Union has proposed a Directive on a Common Framework for Electronic Signatures for

8. Information Security Committee, Electronic Commerce Division, *Digital Signature Guidelines*, 1996 A.B.A. SEC. SCI. & TECH. [hereinafter *Digital Signature Guidelines*], available at <http://www.abanet.org/settach/ec/isc/dsgfree.html/>.

9. *See* UTAH CODE ANN. §§ 46-3-101 to 46-3-504 (1999).

10. *See* CAL GOV'T CODE § 16.5 (West 1999).

11. *See* McBride Baker & Coles, *Hot Topics*, (visited Apr. 9, 1999) <http://www.mbc.com> (providing a regularly updated summary of all enacted and pending electronic and digital signature legislation). Massachusetts is the only state that has not introduced any e-commerce legislation). *Id.*

12. *See* McBride Baker & Coles, *Summary of Electronic Commerce and Digital Signature Legislation* (visited Apr. 12, 1999) <http://www.mbc.com/ds_sum.html>.

13. The UETA project was completed in Spring 1999 and will be ready for approval by NCCUSL at its annual meeting in the Summer of 1999. Accordingly, the UETA should be ready for enactment by the states in early 2000.

the European Union;[14] and the United Nations Commission on International Trade Law ("UNCITRAL") Working Group on Electronic Commerce[15] completed work on its Model Law on Electronic Commerce[16] in 1996, and is currently drafting international legislation addressing digital signatures and certification authorities.[17] The Organization for Economic Co-operation and Development ("OECD") is also addressing electronic signature legal issues,[18] as are several other public and private organizations.[19]

Yet a quick look at the electronic signature legislation currently enacted or under consideration[20] reveals that while there is agreement on where we ultimately want to go (facilitating e-commerce), there is little agreement on how to get there. As discussed in more detail below, legis-

---

14. *See* European Commission, *supra* note 6, at 1.

15. UNCITRAL: THE UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (2d ed. 1991). UNCITRAL is the body within the United Nations primarily charged with oversight of international commercial law. It was created in 1966 by General Assembly Resolution 2205 (XXI) in order to enable the United Nations to play a more active role in reducing or removing legal obstacles to the flow of international trade. A list of its completed projects and their current status may be found at UNCITRAL's home page <http://www.un.or.at/uncitral>.

Amelia H. Boss, *Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform*, 72 TULANE L. REV, 1932 n.3 (1998).

16. *See* United Nations, *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment* 1996 (visited Apr. 19, 1999) <www.un.or.at/uncitral/english/texts/electcom/ml-ec.htm>.

17. In 1996, UNCITRAL decided to place the issues of digital signatures and certification authorities on its agenda. UNCITRAL's Working Group on Electronic Commerce was requested to examine the desirability and feasibility of preparing uniform rules on those topics, and to provide UNCITRAL with sufficient elements for an informed decision regarding the scope of the uniform rules to be prepared. As to a more precise mandate for the Working Group, it was agreed that the uniform rules should address such issues as: the legal basis supporting certification processes, including emerging digital authentication and certification technology; the applicability of the certification process; the allocation of risk and liabilities of users, providers, and third parties using certification techniques; the specific issues of certification through the use of registries; and incorporation by reference. *See* United Nations Commission on International Trade Law, *Report of the Working Group on Electronic Commerce on the Work of its Thirty-Second Session* (Feb. 11, 1998) <http://www.un.or.at/uncitral/english/sessions/unc/unc-31/acn9-446.htm>.

18. *See* Organisation for Economic Co-operation and Development, *EMU—Facts, Challenges and Policies* (last modified Mar. 16, 1999) <http://www.oecd.org>. The OECD is an international organization with twenty-nine member countries from North America, Europe, and the Asia-Pacific area. Based in Paris, France, OECD is a forum permitting governments of the industrialized democracies to study and formulate economic and social policies. Its sole function is direct cooperation among the governments of its member countries. *Id.*

19. *See, e.g.*, ILPF, *Internet Law and Policy Forum* (visited Apr. 9, 1999) <http://www.ilpf.org>.

20. *See* McBride Baker & Coles, *supra* note 12 (providing a summary of all electronic and digital signature legislation).

lation ranges from a minimalist approach that simply authorizes the use of electronic signatures in very limited circumstances, to legislation that establishes some evidentiary presumptions and default provisions that parties can contract out of, to a very formal and highly regulatory approach governing the manner in which digital signatures may be used and certification authorities may operate.[21]

The essential question with regard to electronic signature legislation is: How far down the road will it take us? Can the various types of legislation move e-commerce in the right direction, or might they cause unintended detours? Should we simply wait for disputes to arise and leave it to judges to transform the legal landscape? Do the laws that work remarkably well and provide predictability in the traditional, paper-based commercial world translate line for line and serve as adequate mile markers for companies blazing trails to more efficient commerce on the new electronic frontier? Given the explosion of e-commerce activity, is legislation even necessary, or are there inherent limits to the growth of e-commerce that legislation could help to overcome?

Enacting legislation designed simply to remove barriers, while an important and worthwhile endeavor, may not move us far enough toward the ultimate goal. Conversely, enacting laws or imposing regulations that force the market to use a specific business model or specific technology, or that protect against perceived problems that have not yet surfaced, might preclude the pursuit of more promising e-commerce avenues.

Yet, if done properly, electronic signature legislation can, and perhaps should, be designed and enacted to accomplish two goals: (1) to *remove barriers* (actual and perceived) to e-commerce, and (2) to *enable* and *promote* the desirable public policy goal of e-commerce by helping to establish the "trust" and the "predictability" needed by parties doing business online. These two goals might be best accomplished by enacting legislation that preserves freedom of contract while recognizing that, because parties don't always resolve all issues by prior contractual agreement, limited default rules should apply when such unresolved issues arise. Although the judiciary will certainly play a key role in establishing the rules that will govern online transactions, we should not automatically discount the positive contributions and early guidance that legislation can provide. Likewise, while the goal of technology neutrality is important from the standpoint of not stifling development or unfairly favoring one technology over another, we must be careful as we draft electronic signature legislation not to let neutrality become an excuse to avoid addressing legitimate new issues raised by a unique technology, or worse, use neutrality as a means to discriminate against the develop-

21. *Id.*

ment of those technologies seen by most as facilitating secure e-commerce. Finally, we must continually be cognizant of the danger that the forty-nine different versions of electronic signature legislation undertaken by the various states in this country might, despite our best intentions, actually undermine the trust and predictability we are seeking to establish.

Toward that end, this article explores some of the questions we should be asking ourselves in using electronic signature legislation as a vehicle for advancing e-commerce.[22] First, we will define what we mean when we refer to electronic and digital signatures. Second, we will examine the three fundamental legal issues raised by online transactions that have fostered the felt need for electronic signature legislation. Furthermore, for each issue, we will outline the underlying concerns, examine the primary legislative approaches developed to date, and discuss the role that electronic signature legislation—whether at the state or federal level—can play in allaying the identified concerns. Third, we will conclude with some thoughts on legislation's role in promoting the growth of e-commerce by reviewing some statutes that have historically been a positive force in promoting economic growth.

II. THE CORE LEGISLATIVE CONCERN: ELECTRONIC AND DIGITAL SIGNATURES

The core concern of electronic signature legislation has been electronic documents, sometimes referred to as "records" or "electronic records,"[23] and "signatures" that are created, communicated, and stored in electronic form.[24] Generally, these signatures are referred to as either "electronic signatures" or "digital signatures." Unfortunately, these terms themselves have created considerable confusion.[25] Thus, for pur-

22. Because our focus is primarily on business-to-business e-commerce, we do not address the additional issues raised by consumers' concerns.

23. *See, e.g.*, 5 ILL. COMP. STAT. 175/5-105 (effective July 1, 1999). Under Illinois law, a "record" is "information that is inscribed, stored, or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." *Id.* Additionally, an "electronic record" is a "record generated, communicated, retrieved, or stored by electronic means for use in an information system or for transmission from one information system to another." *Id. See also* Report of the United Nations Commission on International Trade Law on The Work of its Twenty-Ninth Session, U.N. GAOR, 51st Sess., Supp. No. 17, at Annex 1, U.N. Doc. A/51/17 (1996).

24. "Electronic" form refers generally to a variety of formats by which information can be stored, including electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to the foregoing technologies. *See, e.g.*, 5 ILL. COMP. STAT. 175/5-105.

25. Because all forms of electronic signatures exist in digital form, many of the electronic signature statutes erroneously use the technology-specific term "digital signature" to refer to the generic class of all methods by which an electronic message can be signed—i.e.,

poses of this article, we will define these terms as most commentators have:[26]

• *"Electronic signature"* is a generic, technology-neutral term that refers to the universe of all of the various methods by which one can "sign" an electronic record. Although all electronic signatures are represented digitally (i.e., as a series of ones and zeroes), they can take many forms and can be created by many different technologies. Examples of electronic signatures include: a name typed at the end of an e-mail message by the sender; a digitized image of a handwritten signature that is attached to an electronic document (sometimes created via a biometrics-based technology called signature dynamics);[27] a secret code or PIN (such as that used with ATM cards and credit cards) to identify the sender to the recipient; a code or "handle" that the sender of a message uses to identify himself; a unique biometrics-based identifier, such as a fingerprint or a retinal scan; and a digital signature (created through the use of public key cryptography).

• *"Digital signature"*[28] is simply a term for one technology-specific type of electronic signature. It involves the use of public key cryptogra-

---

electronic signatures. Some statutes correctly use the term "digital signature" to refer to a public key cryptography-based signature, while other statutes use it to refer to any type of signature in digital form (i.e., an "electronic signature"). Statutes in this latter category include: ARIZ. REV. STAT. ANN. § 41-132 (West 1998); CAL. GOV'T CODE § 16.5 (West 1999); GA. CODE ANN. § 10-12-4 (Michie 1998); 15 ILL. COMP. STAT. 405/14.01 (West 1998); MD. CODE ANN. STATE GOV'T § 8-504 (1998); NEB. REV. STAT. ANN. § 86-170 (Michie 1999); N.H. REV. STAT. ANN. § 294-D: 4 (1999); TEX. GOV'T CODE ANN. § 2054.060 (West 1999); TEX. TRANSP. CODE ANN. § 201.933 (West 1999); VA. CODE ANN. §§ 59.1-467, 59.1-468, 59.1-469 (Michie 1998). *See e.g.*, CAL GOV'T CODE § 16.5 (defining a "digital signature" as "an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature"). *Cf.* FLA. STAT. § 282.70 (West 1998) (defining an "electronic signature" more appropriately as "any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing").

26. Global Information Infrastructure Commission, *A Global Action Plan for Business With Governments Toward Electronic Commerce* (Sept. 9, 1998 draft) <http://www.giic.org/pubs/e_biaa.pdf>. A consensus appears to be emerging to define "electronic signature" as the process of signing an electronic document or transaction to obtain legal equivalence with the hand written signature, and "digital signature" as one (but not the only) technique to deliver the functions required of an electronic signature. *Id.*

27. CAL. CODE REGS. tit. 2 § 22003(b)(1)(D) (1998). Under the California Digital Signature Regulations, "'Signature Dynamics' means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques." *Id.*

28. For purposes of this article, we assume that the reader is familiar with digital signatures and the asymmetric (public key) cryptography used to create them. For an overview of this technology and the process by which digital signatures are created; *see* THOMAS J. SMEDINGHOFF, ONLINE LAW chs. 3, 4, 31 (1996); WARWICK FORD AND MICHAEL BAUM, SECURE ELECTRONIC COMMERCE (1997); *Digital Signature Guidelines*, *supra* note 8.

phy[29] to "sign" a message,[30] and is perhaps the one type of electronic signature that has generated the most business and technical efforts, as well as legislative responses.

A signature, whether electronic or on paper, is first and foremost a *symbol* that signifies *intent*. Thus, the definition of "signed" in the Uniform Commercial Code includes "any symbol" so long as it is "executed or adopted by a party with present *intention* to authenticate a writing."[31] The primary focus, of course, is on the "intention to authenticate," which distinguishes a signature from an autograph. Yet, the nature of that intent will vary with the transaction, and in most cases can be determined only by looking at the context in which the signature was made.[32] A signature may, for example, signify an intent to be bound to the terms of the contract, the approval of a subordinate's request for funding of a project, confirmation that a signer has read and reviewed the contents of a memo, an indication that the signer was the author of a document, or merely that the contents of a document have been shown to the signer and that he or she has had an opportunity to review them.

In addition to evidencing a person's intent, a signature can also serve two secondary purposes. First, a signature may be used to identify the person signing. Second, a signature may serve as some evidence of the integrity of a document, such as when parties sign a lengthy contract on the final page and also initial all preceding pages to guard against alterations in the integrity of the document through a substitution of pages.

For electronic transactions, these secondary signature functions of identity and integrity can be key. Especially to the extent that we automate electronic transactions, and conduct them over significant distances using easily altered digital technology, the need for a way to ensure the identity of the sender and the integrity of the document becomes pivotal.

Unlike the world of paper-based commerce, where the requirement of a signed writing most frequently serves the function of showing that an already identified person made a particular promise, in the e-com-

29. Public key cryptography employs an algorithm using two different but mathematically related cryptographic keys. One key is for creating a digital signature or transforming data into a seemingly unintelligible form, and the other key is for verifying a digital signature or returning the message to its original form.

30. In more technical terms, a digital signature is the sequence of bits that is created by running an electronic message through a one-way hash function to create a unique digest (or "fingerprint") of the message and then using public key encryption to encrypt the resulting message digest with the sender's private key.

31. U.C.C. § 1-201(39) (1999).

32. Some statutes, however, infer intent. *See, e.g.*, CCA, *Singapore Electronic Transactions Act 1998*, §18(2)(b) <http://www.cca.gov.sg/eta/framecontent.htm> [hereinafter *Singapore Electronic Transactions Act*].

merce world, a requirement of an authenticated electronic message serves not only this function, but the more fundamental function of identifying the person making the promise contained in the message in the first place. This additional function is critical in e-commerce because there are few other methods of establishing the source of an electronic message.[33]

Thus, while handwritten signatures in most cases serve merely to indicate the signer's intent, signatures in an electronic environment typically serve three critical purposes for the parties engaged in an e-commerce transaction—i.e., to identify the sender,[34] to indicate the sender's intent (e.g., to be bound by the terms of a contract), and to ensure the integrity of the document signed.[35]

III. THE FUNDAMENTAL LEGAL ISSUES RAISED BY E-COMMERCE

Three fundamental legal issues arise when parties to a transaction use electronic records to replace paper, employ an electronic medium as the mode of communication, and use electronic signatures to authenticate their transactions:

• *Is it legal?* Both federal and state law contain many requirements that transactions be documented in "writing" and be "signed." Many are concerned that this requires ink on paper and, thus, that electronic communications do not meet appropriate legal requirements for writing and signature and will not be enforceable.

• *Can I trust the message?* Recipients of electronic messages must have some basis for trusting the message (from a legal perspective), so that they can act in reliance upon the message, often in real time, and without the need for out-of-band verification communications. Achieving the key goals of e-commerce (including speed, efficiency, and economy) requires that recipients of electronic messages be willing to act in reliance on messages received (e.g., ship product, transfer funds, enter into binding contractual commitments, change position in reliance on messages), and to do so promptly and in many cases automatically. Yet, the indicia of reliability that usually accompany paper-based communi-

33. R. J. Robertson, Jr., *Electronic Commerce on the Internet and the Statute of Frauds*, 49 S.C. L. REV. 813 (1998).

34. *See infra* notes 60-65 and accompanying text. In apparent recognition of this fact, the electronic signature statutes enacted in several states (e.g., California) require that an electronic symbol identify the signer before that symbol will qualify as an electronic signature.

35. It is, of course, possible to use a security procedure to preserve the integrity of an electronic record without creating an electronic signature. Yet, regardless of whether an electronic signature or an alternative security procedure is used, the issue of ensuring the integrity of electronic documents must be addressed.

cations (such as a paper document signed with ink signatures and delivered by trusted third parties such as the U.S. Postal Service) are missing in electronic transactions. Moreover, the ease with which digital documents can be altered without detection increases the risk of fraud for electronic transactions.

• *What are the rules of conduct?* As with all legal transactions, the parties should know the rules of the game. For example, what is the liability of a certification authority or a trusted third party for inaccurate identification? What is the liability of the signer of a message who loses the private key or other signature device used to create the message? What is required for cross-border recognition of electronic messages?

The most difficult question of all is what role, if any, electronic signature legislation should play in addressing such legal issues. The following sections will explore these three legal issues, the extent to which electronic signature legislation addresses these issues, and the direction in which such legislation should be moving.

A. Is It Legal? Removing Barriers to Electronic Commerce

1. *The Issue*

The first of these three issues—is e-commerce legal?—is the most fundamental, because it involves questions regarding the enforceability of electronic transactions. This issue raises concerns regarding whether electronic records and electronic signatures meet legal formalities such as the writing and signature requirements imposed by a variety of statutes and regulations; whether an electronic record constitutes an "original" for evidentiary purposes;[36] whether electronic records and electronic signatures will be denied admissibility because of their electronic form;

36. The requirement that a document be "an original" occurs in a variety of contexts for a variety of reasons. In many situations, documents must be transmitted unchanged (i.e., in their "original" form), so that other parties may have confidence in their contents. Examples of documents where an "original" is often required include trade documents (e.g., weight certificates, agricultural certificates, quality/quantity certificates, inspection reports, insurance certificates) and non-business related documents (e.g., birth certificates and death certificates). When these documents exist on paper, they are usually only accepted if they are "original," because alterations may be difficult to detect in copies.
The requirement that a document be "an original" is also important from an evidentiary perspective. In particular, the "best evidence rule," sometimes referred to as the "original document rule," requires that: "[i]n proving the terms of a writing, where the terms are material, the original writing must be produced unless it is shown to be unavailable for some reasons and other than the serious fault of the proponent." Edward W. Cleary, McCormick on Evidence § 230 at 704 (3d ed. 1984). *See also* 6 Jack B. Weinstein's Federal Evidence § 1002 (Joseph M. McLaughlin & Matthew Bender eds., 2d ed. 1998) (defining "Requirement of Original," which states that "to prove the content of a writing, recording or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by act of Congress").

whether records can be maintained solely in an electronic form; and whether the recordkeeper can establish the authenticity and integrity of such records.

Yet, the concern that has generated the most discussion, and the one that we examine here, is whether electronically signed records meet writing and signature requirements. In many cases, the law requires that an agreement be both documented in "writing,"[37] and "signed" by the person who is sought to be held bound, in order for that agreement to be enforceable. The Statute of Frauds is, of course, the best example of such a law.[38] Nevertheless, thousands of other federal, state, and local statutes and regulations also require a transaction to be documented by a writing and a signature. In Illinois, for example, over 3,000 statutory sections contain such requirements. Likewise, Georgia has over 5,500, and Ohio has over 8,000, such statutory sections.[39]

Statutes and regulations that require transactions to be "in writing" and "signed" are generally perceived to constitute barriers to e-commerce—barriers that must be removed if e-commerce is to flourish. Otherwise, an electronic record might not satisfy statutory writing requirements, and an electronic signature might not satisfy statutory signature requirements. In other words, there is a concern that writing and signature requirements are satisfied only by ink on paper. Interestingly, however, concerns over whether electronic records and electronic signatures will satisfy these legal requirements may not be warranted.[40] As

37. Requirements that agreements be "in writing" serve a variety of purposes. These include: (1) providing tangible evidence of the existence and nature of the intent of the parties to bind themselves; (2) alerting parties to the consequences of entering into a contract; (3) providing a document that is legible to all, including strangers to the transaction; (4) providing a permanent record of the transaction that remains unaltered over time; (5) allowing the reproduction of a document so that each party can have a copy of the same; (6) allowing for the authentication of the data by means of a signature; (7) providing a document that is in a form acceptable to public authorities and courts; (8) finalizing the intent of the author of the writing and providing a record of that intent; (9) allowing easy storage of data in tangible form; (10) facilitating control and subsequent audit for accounting, tax, or regulatory purposes; and (11) bringing legal rights and obligations into existence in those cases where a "writing" is required for validity purposes. *See* Commission on Electronic Commerce and Crime, *Final Report of the Commission on Electronic Commerce and Crime* (Mar. 23, 1998) <http://www.mbc.com/ceccmsg.html>.

38. For the Statute of Frauds and contracts involving the sale of goods, see U.C.C. § 2-201(1) (1998); *see also* U.C.C. § 1-206 (1998) (limiting enforcement of unsigned, unwritten contracts for the sale of securities for $5,000 or more). See RESTATEMENT (SECOND) OF CONTRACTS, § 110 statutory note, at 284-85 (1982) for a state-by-state listing of state statutes of frauds.

39. *See* Report of the National Conference of Commissioners on Uniform State Laws (NCCUSL), *Uniform Electronic Transactions Act, Task Force on State Law Exclusions* (Sept. 18, 1998), <http://www.webcom.com/legaled/ETAForum/docs/report4.html>.

40. *See* Letter from Business Software Alliance, to Professor Raymond T. Nimmer & Carlyle C. Ring, Jr., *Article 2B Drafting Committee* (Jan. 20, 1999) <http://

the discussion below indicates, the case law suggests that courts would find that electronic records can meet the statutory writing requirements, and that electronic signatures can meet the statutory signature requirements.

a. Writing Requirement

The traditional definition of a "writing" is not limited to ink on paper. Rather, the essence of the requirement is that the communication be reduced to a tangible form.[41] As early as 1869, a New Hampshire court found a telegraphed contract to be a sufficient writing under the Statute of Frauds:

> It makes no difference whether that operator writes the offer or the acceptance . . . with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by use of the finger resting upon the pen; nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office.[42]

Courts have also found telexes, Western Union Mailgrams, and even tape recordings to be writings under the Statute of Frauds.[43] Faxes have been assumed to be writings under the Statute of Frauds.[44] Magnetic recordings of data on computer disks have been held to constitute "writings" for a variety purposes, including under forgery statutes and copyright law.[45] Accordingly, it is likely that a court would find that

---

www.2bguide.com/docs/0199bsa.html>. According to the Business Software Alliance, "billions of dollars of business is being successfully conducted on an assumption of nondiscrimination [against electronic records and signatures] and there are no reported decisions that could be fairly construed as systematically discriminating against electronic records or signatures in the context of contract law issues." *Id.*

41. The U.C.C. defines "written" or "writing" as "printing, typewriting or *any other intentional reduction to tangible form.*" U.C.C. § 1-201(46) (1998) (emphasis added).

42. Howley v. Whipple, 48 N.H. 487 (1869). One commentator has noted that "the Whipple opinion was a bit eccentric in its metaphors, to be sure, but was not maverick in its results." Douglas Morrison, Note, *The Statute of Frauds Online: Can a Computer Sign a Contract for the Sale of Goods*? 14 GEO. MASON U. L. REV. 637 (1992).

43. Joseph Denunzio Fruit Co. v. Crane, 79 F. Supp. 117 (S.D. Cal. 1948) (holding that a telex is a writing); McMillan Ltd. v. Weimer Drilling & Eng. Co., 512 So.2d 14 (Ala. 1986) (holding that a mailgram is a writing); Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212 (D. Colo. 1972) (holding that a tape recording is a writing). *But see* Roos v. Aloi, 127 Misc.2d 864 (N.Y. Sup. Ct. 1985) (holding that a tape recording is not a writing).

44. *See* Bazak Int'l Corp. v. Mast Indus., Inc., 535 N.E.2d 633 (N.Y. 1989) (assuming faxes to be writings under U.C.C. 2-201). In *American Multimedia Inc. v. Dalton Packaging, Inc.*, 143 Misc.2d 295 (N.Y. Sup. Ct. 1989), a faxed purchase order was assumed to be a writing for purposes of a federal arbitration statute.

45. People v. Avila, 770 P.2d 1330 (Colo. Ct. App. 1988) (stating that recording on computer disk was a "writing" for purposes of forgery statute). *See also* Clyburn v. Allstate, 826 F. Supp. 955 (D.S.C. 1993).

electronic messages recorded in a tangible medium would also satisfy the writing requirement.[46]

b. Signature Requirement

Generally, a signature is "any symbol executed or adopted by a party with present intention to authenticate a writing."[47] Thus, the key requirement is not ink on paper, but rather the presence of a "symbol" coupled with the party's "intention."

The courts have found many symbols on a variety of media to be signatures: names on telegrams,[48] names on telexes,[49] typewritten names,[50] names on Western Union Mailgrams,[51] and even names on letterhead.[52] Faxed signatures have also been assumed to constitute effective signatures.[53] Thus, any symbol or code on an electronic record that

46. Some courts may have concerns about reliability—i.e., whether magnetic media are more subject to tampering than paper—but these concerns should not affect whether an electronic transmission is considered a writing. Rather, they should only be relevant to the authentication, for evidence purposes, of a particular transmission record. *But see* Morrison, *supra* note 42, at 637 (analyzing reliability of EDI records in determining whether to consider them "writings" under the Statute of Frauds).

47. U.C.C. § 1-201(39) (1998).

48. Selma Savings Bank v. Webster County Bank, 206 S.W. 870 (Ky. 1918); Hillstrom v. Gosnay, 614 P.2d 466 (Mont. 1989). *But see* Pike Indus., Inc. v. Middlebury Assoc., 398 A.2d 280 (Vt. 1979); *aff'd on other grounds*, 436 A.2d 725 (Vt. 1980), *cert denied*, 455 U.S. 947 (1992). *See* Morrison, *supra* note 42, at 637.

49. Joseph Denunzio Fruit Co. v. Crane, 70 F. Supp. at 117; Franklin County Coop. v. MFC Services, 441 So.2d 1376 (Miss. 1983); Hideca Petroleum Corp. v. Tampimac Oil Int'l Ltd., 740 S.W.2d 838 (Tex. Ct. App. 1987). *But see* Miller v. Wells Fargo Bank Int'l Corp., 406 F. Supp. 452 (S.D.N.Y. 1975) (suggesting that there was a question as to whether test key on telex is a signature).

50. In *Watson v. Tom Growney Equip. Inc.*, 721 P.2d 1302 (N.M. 1986), a name typed on a purchase order was found to be a sufficient signature, because the signatory had deliberately filled out other details on the form. *See In re* Matter of Save-On Carpet of Arizona, Inc., 545 F.2d 1239 (9th Cir. 1976) (holding that a typewritten signature on a U.C.C. financing statement satisfied the signature requirement of the Statute of Frauds). *But see In re* Carlstrom, 3 U.C.C. Rep. Serv. 766 (Bk. D. Me. 1966). *See also* A & G Const. Co. v. Reid Bros. Logging Co., 547 P.2d 1207 (Alaska 1976) (holding that a typed name was sufficient).

51. Hesenthaler v. Farzin, 564 A.2d 990 (Pa. Super. Ct 1989) (focusing on intent to authenticate); McMillan Ltd v. Warrior Drilling & Eng Co., 512 So. 2d 14 (Ala. 1986).

52. In *Kohlmeyer & Co. v. Bowen*, 192 S.E.2d 400 (Ga. Ct. App. 1972), a securities brokerage firm's name was printed on a confirmation statement for the sale of securities. The court found that the printed name was intended as authentication and met the signature requirement under the Statute of Frauds. *See also* Associated Hardware Supply Co. v. Big Wheel Distrib. Co., 355 F.2d 114 (3d Cir. 1966) (discussing printed names on letterhead).

53. In *Beatty v. First Exploration Fund 1987 and Co. Limited Partnership*, 25 B.C.L.R.2d 377 (1988), a British Columbia case, faxed signatures on proxy documents were sufficient to meet the signature requirements under a limited partnership agreement. In *Gilmore v. Lujan*, 947 F.2d 1340 (9th Cir. 1991), the court upheld an agency's determina-

is intended as a signature should also meet the requirement. Even a name typed at the end of an e-mail should qualify as a signature,[54] so long as it was created with the proper intent.

Yet, concerns have lingered not only because of a few contrary court decisions,[55] but also because of a lack of specific statutory authorization. Notwithstanding the foregoing case law, a general concern about the "legality" of electronic records and electronic signatures has persisted, leading to numerous calls for legislation to remove the perceived barriers to e-commerce resulting from traditional writing and signature requirements. The benefits of predictability in the law[56] argue in favor of legislation that clearly and unambiguously states that electronic signatures satisfy legal signature requirements and that electronic records can satisfy legal writing requirements.

2. *The Legislative Response*

All electronic signature statutes enacted to date have a component designed to remove these perceived barriers to e-commerce. In fact, for most electronic signature legislation, that is the only issue that is addressed.

Unfortunately, the legislative approaches to what appears to be a simple issue of merely removing barriers to e-commerce have been somewhat varied and inconsistent, and may have actually made the situation worse. Specifically, in clarifying that electronic records meet writing requirements and that electronic signatures meet signature requirements, statutes have differed greatly regarding two fundamental issues: (1) What qualifies as a signature; and (2) what types of transactions can be undertaken using electronic records and electronic signatures. The following sections discuss the variety of legislative approaches (and inconsistencies) regarding these two issues.

a. What Qualifies as a Signature?

Perhaps the biggest issue that arises in legislation devoted to removing barriers to e-commerce is the question of what type of electronic signature qualifies as a signature (i.e., meets statutory and regulatory signature requirements). Unfortunately, there is no uniform answer to

---

tion that a fax did not meet the regulation's strict requirement that a document be "holographically signed in ink," but criticized the agency for its narrow-minded approach. In *Madden v. Hegadon*, 565 A.2d 725 (N.J. Super. 1989), *aff'd* 571 A.2d 296 (N.J. 1989), a faxed signature was deemed effective for filing a nomination petition.

54. *See* BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE (1994).

55. *See, e.g.*, Department of Trans. v. Norris, 474 S.E.2d 216 (Ga. Ct. App. 1996), *rev'd sub nom.*, Norris v. Georgia Dep't of Trans., 486 S.E.2d 826 (Ga. 1997) (holding that a fax transmission was not a writing).

56. *See* discussion *infra* Section C.3.

this question. Typically, legislation has taken one of three apparently inconsistent approaches: (1) all electronic signatures satisfy legal signature requirements; (2) electronic signatures satisfy legal signature requirements only when they possess certain security attributes; or (3) digital signatures satisfy legal signature requirements.

Moreover, not only is legislation inconsistent from state to state, but in some cases inconsistent approaches have been enacted within the same state.

In the paper world, at least in the United States, anything can qualify as a signature. The current definition of signature in the Uniform Commercial Code ("U.C.C.") includes "*any symbol* made with an intent to authenticate."[57] Because there is no requirement as to the nature of the mark that qualifies, courts have found that, in addition to the traditional handwritten signature, a wide variety of marks (including a simple "X") will qualify.[58] Several states have taken the same approach with electronic signatures—that is, any form of electronic "symbol" on a message can qualify as a signature.[59] All such statutes take a technology-neutral

57. U.C.C. § 1-201(39) (1999) (emphasis added).

58. *See* notes 47-56 and accompanying text.

59. *See* ARIZ. REV. STAT. ANN. § 41-132(D)(4) (West 1998) (defining electronic signature as an "electronic or digital method of identification that is executed or adopted by a person with the intent to be bound by or to authenticate a record"); FLA. STAT. ANN. § 282.72(4) (West 1998) ("Electronic signature means any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing."); 5 ILL. COMP. STAT. 175/5-105 (effective July 1, 1999) ("[A]ny symbol executed or adopted, or any security procedure employed or adopted, using electronic means or otherwise, by or on behalf of a person with intent to authenticate a record."); IND. CODE ANN. § 5-24-2-2 (West 1998) ("[A]n electronic identifier, created by computer, executed or adopted by the party using it with the intent to authenticate a writing."); MISS. CODE ANN. § 25-63-1 (1998) ("[A]ny word, group of letters, name, including a trader-assumed name, mark, characters or symbols made manually, by device, by machine, or manifested by electronic or similar means, executed or adopted by a party with the intent to authenticate a writing."); N.H. REV. STAT. ANN. § 506:8 (1999) ("Electronic signature means a digital signature, executed or adopted by a party with an intent to authenticate a writing."); OHIO REV. CODE ANN. § 3701.75

> ("[A]ny of the following attached to or associated with an electronic record by an individual to authenticate the record: (a) a code consisting of a combination of letters, numbers, characters, or symbols that is adopted or executed by an individual as that individual's electronic signature; (b) a computer-generated signature code created for an individual; (c) an electronic image of an individual's handwritten signature created by using a pen computer.");

OR. REV. STAT. § 192.835 (1998) ("[A]ny letters, characters or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing."); S.C. CODE ANN. § 26-5-330 (Law. Co-op. 1998) ("[A]ny identifier or authentication technique attached to or logically associated with an electronic record that is intended by the party using it to have the same force and effect as a manual signature."); TEX. BUS. & COM. CODE ANN. § 2.108 (West 1998) ("[A]n electronic identifier, created by a computer, intended by the party using it to have the same force and effect as the use of a manual

approach to the means by which such signatures are created (i.e., they do not specify the technology that must be used, only the result that must be achieved). The only requirements are, quite simply, the existence of a symbol or security procedure, and an intent to authenticate on the part of the signer. The proposed Uniform Electronic Transactions Act also takes this approach.[60]

A second category of statutes, however, requires that electronic signatures possess certain attributes or meet certain requirements before they will be considered legally enforceable. Virtually all of these statutes take a technology-neutral approach to these requirements.

Perhaps the most common requirements imposed by this second category of statutes derive from a decision of the U.S. Comptroller General that was first included in the California legislation enacted in late 1995.[61] Under statutes adopting this approach, an electronic signature is legally effective as a signature only if it is: (1) unique to the person using it; (2) capable of verification; (3) under the sole control of the person using it; and (4) linked to the data in such a manner that if the data is changed, the signature is invalidated. Some statutes have varied this approach by including these four requirements in the definition of an electronic signature (i.e., it's not an electronic signature if it doesn't possess those four attributes) but also specifying that only electronic signatures are legally effective as signatures. In either case, however, this approach requires attributes of security as a precondition to the validity of the signature itself, something not required for paper-based signatures. Statutes in nearly a third of the states have adopted this approach.[62] The draft European Directive takes a similar approach.[63]

---

signature."); VA. CODE ANN. §§ 59.1-467, 59.1-468, 59.1-469 (Michie 1998) ("[A]n electronic identifier, created by a computer, intended by the party using it to have the same force and effect as the use of a manual signature."); W. VA. CODE § 39-5-2 (e) (1998) ("[A]ny identifier or authentication technique attached to or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a manual signature."); WIS. STAT. ANN. § 137.04(2) (West 1999) ("[A]ny combination of words, letters, symbols or characters that is attached to or logically associated with an electronic record and used by a person for the purpose of authenticating a document that has been created in or transformed into an electronic format.").

60. *See* Uniform Transactions Act, § 102(8) (May 10, 1999 interim draft) (on file with author).

61. *See* U.S. Comptroller General, *Matter of National Institute of Standards and Technology: Use of Electronic Data Interchange Technology to Create Valid Obligations*, 71 Comp. Gen. 109 (1991); (Dec. 13, 1991); CAL. GOV'T. CODE § 16.5 (West 1999).

62. *See* ALASKA STAT. § 09.25.510 (Michie 1999) (applying generally to all communications); CAL. GOV'T CODE § 16.5 (limiting application to communications with public entities); GA. CODE ANN. § 10-12-4 (Michie 1998) (applying generally to all communications); IDAHO CODE § 67-2357 (1998) (limiting application to the filing and issuing of documents by and with state and local agencies); 15 ILL. COMP. STAT. 405/14.01 (limiting application to communications between a state agency and the comptroller); 205 ILL. COMP. STAT. 705/5

Unfortunately, the meaning of these four requirements is not entirely clear, and such requirements may create significant and unnecessary hurdles.[64]

(West 1998) (limiting application to communications between financial institutions and their customers); IOWA CODE ANN. § 1555A. 27 (West 1999) (limiting application to prescriptions); KAN. STAT. ANN. § 60-2616 (1997) (applying generally to all communications); KY. REV. STAT. ANN. § 369.020 (Banks-Baldwin 1999) (applying generally to all kinds of communications); MD. CODE ANN. STATE GOV'T § 8-504 (1998) (limiting application to any communications among governmental entities); NEB. REV. STAT. § 86-1701 (1998) (applying generally to all communications); N.H. REV. STAT. ANN. § 294-D:4 (1999) (limiting application to communications between the state and any agency or instrumentality of the state); N.C. GEN. STAT. § 66-58.1 (1999) (limiting application to filings with public agencies); OKLA. STAT. ANN. tit. 15 § 965 (West 1999) (applying generally to all communications); R.I. GEN. LAWS § 42-127-4 (1998) (limiting application to transactions between public agencies).

63. *See* European Commission, *supra* note 6. However, the draft European Directive does not require that these elements be present in order to create an enforceable electronic signature.

64. The four requirements generally impose conditions not normally required to create an enforceable signature on a paper document. They can be explained as follows:

(a) *Unique to the Person Using It*—The requirement that an electronic signature be "unique to the person using it" is presumably intended to ensure that not more than one person would produce the same electronic signature. It is likely that a digital copy of a handwritten signature would be considered to be unique to the individual signer—i.e., every person presumably has a unique way of writing his or her signature. Likewise, the requirement of uniqueness could also presumably be satisfied by a biometric-based signature that incorporates certain attributes unique to the signer, such as a fingerprint or a retinal scan. The requirement can also be satisfied by a digital signature where the public-private key pair used by the signer was randomly generated and of sufficient key length so that the likelihood of anyone else generating the same public-private key pair would be exceedingly remote. By contrast, however, while the name "John Smith" or the letter "X" typed at the bottom of a paper document can qualify as a signature, it is not unique to any person that uses this method of signature, and thus would presumably not qualify as an electronic signature.

Such an absolute requirement of uniqueness is not necessary. If the law of signatures in the context of paper-based transactions does not require that signatures be unique, it may not be appropriate to impose such a requirement on electronic transactions (in certain situations, the recipient of the message may be taking a risk that it cannot authenticate the signature in court, but the recipient takes a comparable risk with a paper-based transaction containing a non-unique signature, such as an "X"). Where uniqueness is required, it seems that it should be required only in the domain in which the signature is used, rather than on a true worldwide basis.

(b) *Capable of Verification*—The requirement that a signature be capable of verification does not mean that the signature itself must consist of or include the signer's name. Rather, it focuses on the ability to determine or verify the identity of the signer of the message. Thus, verification based on reference to other sources of information is likely to be sufficient. For example, under the California Digital Signature Regulations, a digital signature is capable of verification if the recipient of the digitally signed document can verify that the document was digitally signed by using the signer's public key to decrypt the message, and a digitized handwritten signature created using signature dynamics is capable of verification if the handwriting measurements can allow a handwriting and document

A different set of legal signature requirements is imposed by the UNCITRAL Model Law. Specifically, the UNCITRAL Model Law requires that:

1. an electronic signature must include a method to identify the signer,

2. an electronic signature must include a method to indicate the signer's approval of the information contained in the message, and

3. the method used must be as reliable as was appropriate for the purpose for which the message was generated or communicated.[65]

A third category of legislation focuses not on the attributes an electronic signature must possess in order to be enforceable as a signature, but rather on the technology used to create the signature itself. Statutes falling within this third category authorize the use of only a specific type of electronic signature (i.e., a digital signature) and ignore the general category of electronic signatures. Such legislation has been enacted in five states: Minnesota, Missouri, New Hampshire, Utah, and

---

expert to access the authenticity of the signature. *See* CAL. GOV'T CODE § 22003 (West 1999).

It should be noted, however that even the conclusion of an expert in handwriting analysis who has compared admitted signatures of the purported signer with the signature in question is at best subjective. *See, e.g.*, U.S. v. Rosario, 118 F.3d 160 (3d Cir. 1997) ("Handwriting analysis is at best an inexact science, and at worst mere speculation itself.").

(c) *Under the Sole Control of the Person Using It*—The California Digital Signature Regulations provide that (1) a digital signature is under the sole control of the person using it when the person who holds the relevant key pair assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure; and (2) a digitized handwritten signature created using signature dynamics is under the sole control of the person using it if the signature digest captures the handwriting measurements and cryptographically binds them to the message and makes it computationally infeasible for the handwriting measurements to be bound to any other message. CAL. GOV'T CODE § 22003. Yet, it is not clear whether this is a proper interpretation of the "sole control" requirement or whether the requirement is appropriate where another party may be "authorized" to execute a signature on behalf of the signer, such as by operating a check writing machine or using the signer's private key with appropriate authorization.

(d) *Linkage to the Data Signed*—The final requirement is that the signature must be linked to the data being signed in a manner such that if the data is altered after the signature is made, the fact of such alteration is disclosed to persons relying on the electronic record. This requirement is critical for a secure signature, because otherwise the electronic signature of one person could be altered to look like the electronic signature of another, or an electronic signature could be simply excised from one electronic record and pasted onto another. *See, e.g.*, Food and Drug Administration Regulations on Electronic Records and Electronic Signatures, 21 C.F.R. § 11.70 (1999) (providing that "electronic signatures . . . . shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means"). It is questionable, however, whether this requirement should apply to "all" electronic signatures, and it surely does not apply to paper documents. *Id.*

65. *See* United Nations, *supra* note 16, at Article VII, subpara. 1.

Washington.[66]

Yet a fourth category of enacted legislation says nothing whatsoever about what constitutes a valid electronic signature.[67]

These inconsistent approaches create a certain level of uncertainty for businesses trying to do e-commerce in multiple jurisdictions, especially if such businesses do not use electronic signatures that comply with requirements in all jurisdictions.

b. What Types of Transactions Are Covered?

Electronic signature legislation has also taken a variety of approaches regarding the types of transactions for which the use of electronic signatures is authorized. Nearly 40% of the states expressly authorize the use of electronic signatures for virtually all transactions.[68] Other states have statutes that authorize the use of electronic signatures only for certain categories of transactions, such as U.C.C. filings, medical records, or motor vehicle records.[69] Some states, however, condition the

66. MINN. STAT. ANN. § 325K.20 (West 1998); MO. ANN. STAT. § 28.657 (West 1999); N.H. REV. STAT. ANN. § 294-D:4 (1999); UTAH CODE ANN. § 46-3-101 (1998); WASH. REV. CODE ANN. § 19.34.900 (West 1998). This legislation does not prohibit (or render unenforceable) the use of any other form of electronic signature, it simply leaves the issue open. *See, e.g.*, UTAH CODE ANN. § 46-3-101 (1998) ("[N]othing in this chapter precludes any symbol from being valid as a signature under other applicable law such as Utah Uniform Commercial Code Section 70A-1-201(39).").

67. The term "electronic signature" is used, but not defined, in the following statutes: CONN. GEN. STAT. ANN. §§ 19(a)-25(a) (West 1999); DEL. CODE ANN. tit. 29 §§ 2706(a), 5942 (1998); LA. REV. STAT. ANN. §§ 32, 2145, 1520, 3733.1 (West 1999); MINN. STAT. ANN. § 221.173 (West 1998); NEV. REV. STAT. ANN. § 239.042 (Michie 1997); TENN. CODE ANN. § 16-1-115 (1998); WYO. STAT. ANN. § 9-1-306 (Michie 1998); VT. CODE R. 26 (1995). In all of these states, there appears to be no other electronic signature legislation defining the term.

68. Statutes that authorize the use of electronic signatures for all types of transactions include: ALASKA STAT. § 09.25.510 (Michie 1999); FLA. STAT. ANN. § 282.72 (West 1998); GA. CODE ANN. § 10-12-4 (Michie 1998); 5 ILL. COMP. STAT. 175 (effective July 1, 1999); KAN. STAT. ANN. § 60-2616 (1997); KY. REV. STAT. ANN. § 369.020 (Banks-Baldwin 1999); MINN. STAT. ANN. § 325K.20 (West 1998) (referring to digital signatures only); MISS. CODE ANN. § 25-63-1 (1998); MO. ANN. STAT. § 28.657 (West 1999) (referring to digital signatures only); NEB. REV. STAT. § 86-1701 (1998); N.H. REV. STAT. ANN. § 294 D:4 (1999); OKLA. STAT. ANN. tit. 15 § 965 (West 1999); OR. REV. STAT. § 192.835 (1998); S.C. CODE ANN. § 26-5-330 (Law. Co-op. 1998); UTAH CODE ANN. § 46-3-101 (1998) (referring to digital signatures only); VA. CODE ANN. §§ 59.1-467, 59.1-468, 59.1-469 (Michie 1998); WASH. REV. CODE ANN. § 19/34/900 (West 1998) (referring to digital signatures only); W.VA. CODE § 39-5-2 (1999); WIS. STAT. ANN. § 137.04(2) (West 1999). Some of these statutes do have limited exceptions, such as for wills. *See, e.g.*, 5 ILL. COMP. STAT. 175/5-120 (effective July 1, 1999).

69. A number of state electronic signature statutes only pertain to specific types of transactions. *See, e.g.*, ALA. CODE § 40-30-5 (1998) (referring to electronic filing of tax returns and other documents with the Department of Revenue); COLO. REV. STAT. ANN. § 4-9-413 (West 1999) (referring to electronic filing of U.C.C. Financing Statements); CONN. GEN. STAT. ANN. § 42a-9-402 (West 1999) (referring to electronic signatures for medical records

authorization to use electronic signatures on the type of party involved in the transaction. For example, some statutes authorize the use of electronic signatures only where both parties are government agencies,[70] while other statutes require at least one of the parties to be a government entity.[71] In yet other states, statutes authorize the use of electronic signatures only for transactions involving a specific private entity,

---

maintained in hospitals); DEL. CODE ANN. tit. 29 § 2706(a), 5942(a) (1998) (referring to certain state documents relating to budget, accounting, and payroll); HAW. REV. STAT. ANN. § 231-8.5 (referring to electronic filing of court documents); IOWA CODE ANN. § 48A.13 (referring to voter registration forms); IOWA CODE ANN. § 155A.27 (West 1999) (referring to prescriptions); LA. REV. STAT. ANN. § 2144 (West 1999) (referring to medical records); ME. REV. STAT. ANN. tit. 29-A, § 1401 (West 1998) (referring to applications under the Motor Vehicle Code); OHIO REV. CODE ANN. § 3701.75 (West 1999) (referring to health care record authorizations). The status in these states of electronic signatures used for other types of transactions is unclear because it has not been addressed by legislation.

70. Several statutes limit the authorization to use electronic signatures to transactions between government agencies. *See* ARIZ. REV. STAT. ANN. § 41-132 (limiting application to use by state agencies, and for the acceptance of documents filed with the Secretary of State); DEL. CODE ANN. tit. 29 § 2706(a), 5942(a) (1998) (limiting application to the use of electronic signatures for certain state documents relating to budget, accounting, and payroll); KY. REV. STAT. ANN. § 369.020 (Banks-Baldwin 1999) (limiting application to the use of electronic signatures by state agencies in determining whether state construction contractors should be released from performance bond); MD. CODE ANN. STATE GOV'T § 8-504 (1998) (limiting application to communications among governmental entities); N.H. REV. STAT. ANN. § 294-D:4 (1999) (limiting application to communications between the state and any agency or instrumentality of the state); R.I. GEN. LAWS § 42-27-4 (1998) (limiting application to transactions between public agencies).

71. Many statutes authorize the use of electronic signatures only for transactions where at least one of the parties is a government entity. *See* ALA. CODE § 4-30-5 (1998) (referring to filing of tax returns and other documents with the Department of Revenue); CAL. GOV'T CODE § 22003 (West 1999) (applying to communications with public entities); COLO. REV. STAT. ANN. (West 1999) (referring to electronic filing of U.C.C. Financing Statements); IDAHO CODE § 67-23-57 (1998) (referring to filing and issuing of documents by and with state and local agencies); IND. CODE ANN. § 5-24-2-2 (West 1998) (referring to transactions with the state); IOWA CODE ANN. § 48A.13 (West 1998) (referring to voter registration forms); ME. REV. STAT. ANN. tit. 29-A §§ 1401, 1205, and 1410 (referring to use in connection with applications under the Motor Vehicle Code); MO. ANN. STAT. § 28.621 (West 1999) (applying to filings with the Secretary of State for certain business organizations); MONT. CODE ANN. §§ 2-15-401, 2-15-404 (1999) (allowing Secretary of State to implement an electronic filing system); NEV. REV. STAT. ANN. § 239.042 (Michie 1997) (referring to financial transactions with the state); N.M. STAT. ANN. § 14-3-15.2 (Michie 1998) (referring to public records and filings); N.C. GEN. STAT. § 66-58.1 (1999) (limiting application to filings with public agencies); N.D. CENT. CODE § 1-08-12 (1997) (limiting application to filings with public agencies); TEX. GOV'T CODE ANN. § 403.027 (West 1998) (limiting application to transactions with the state comptroller or between public agencies); WYO. STAT. ANN. § 9-1-306 (Michie 1998) (limiting application to filings with the Secretary of State). The status of electronic signatures used for other types of transactions is unclear because it has not been addressed by legislation.

such as a financial institution.[72]

3. *The Role of Legislation in Removing Barriers*

Taking such varied approaches to what qualifies as an electronic signature, what types of transactions can be undertaken electronically, and what types of parties may use electronic signatures may only be making matters worse for e-commerce. For example, one problem created by statutes that authorize the use of electronic signatures only for transactions involving certain types of parties, or only for certain types of transactions, is that it raises a concern that, by implication, any other use of electronic signatures is not authorized. By providing for the enforceability of electronic signatures in certain limited types of transactions, the legislature may have implicitly evidenced an intention to preclude the enforceability of electronic signatures in other types of transactions. To put it another way, we would not need specific legislation authorizing the use of electronic signatures if electronic signatures were generally enforceable. And, of course, when different states set different standards as to what attributes are required for an electronic signature before it will be considered enforceable, businesses face daunting practical difficulties in using electronic signatures for transactions on a nationwide (not to mention a worldwide) basis.

The bottom line is that in trying to remove barriers, we may have created more uncertainty. While there may be disagreement on the proper definition of an electronic signature, or on exactly which types of transactions are not appropriately conducted by electronic means, the lack of uniformity between the states may be creating a more significant barrier to e-commerce.

B. CAN I TRUST THE MESSAGE?

1. *The Issue*

The second primary concern of parties to an electronic transaction is the issue of trust. That is, what is required before a party will act in reliance on electronic messages in real time, and enter into commercial transactions, ship product, extend credit, transfer funds, change the party's position, or otherwise enter into binding legal commitments with significant economic consequences? The importance of trust for the success of e-commerce is widely recognized. For example, the Commission of the European Communities noted that:

> The first objective is to build trust and confidence. For e-commerce to develop, both consumers and businesses must be confident that their

72. *See, e.g.*, the Illinois Financial Institutions Digital Signature Act of 1999, 1997 H.B. 597 (arguably superceded by 5 ILL. COMP. STAT. 175 (effective July 1, 1999).

> transaction will not be intercepted or modified, that the seller and the buyer are who they say they are, and that transaction mechanisms are available, legal, and secure. Building such trust and confidence is the prerequisite to win over businesses and consumers to e-commerce.[73]

Likewise, the world's largest software industry trade association observed that: "[t]he notion of trust in e-commerce is of critical importance and applies to both consumers and businesses. From secure sales to the handling of personal data to certifying transactions and individuals, trust is the underlying issue that will determine whether e-commerce reaches its full potential."[74]

Trust, of course, plays a role in virtually all commercial transactions. Regardless of whether the deal is struck in cyberspace or in the more traditional paper-based world, transacting parties must trust the messages that form the basis for the bargain. Trusting a message, from a legal perspective, requires consideration of the authenticity and integrity of the message, as well as an assessment of whether the message is nonrepudiable by the sender in the event of a dispute.

a. Authenticity

Authenticity is concerned with the source or origin of a communication.[75] Who sent the message? Is it genuine or a forgery?

A party entering into an online transaction in reliance on an electronic message must be confident of that message. For example, when a bank receives an electronic payment order from a customer directing that money be paid to a third party, the bank must be able to verify the source of the request and ensure that it is not dealing with an impostor.[76]

Likewise, a party must also be able to establish the authenticity of its electronic transactions should a dispute arise. That party must re-

---

73. Commission of the European Communities, *A European Initiative in Electronic Commerce* COM (97) 157 (Apr. 16, 1997 final draft) <http://www.cordis.lu/esprit/src/ecomcom.htm>.

74. Software Publishers Association (n/k/a Software and Information Industry Association), *Code, Content and Commerce: SPA's Vision for the Digital Future* (May, 1998) <http://www.spa.org/govmnt/govnews.htm>.

75. *See* FED. R. EVID. 901(a) (1995).

76. *See* U.C.C. §§ 4A-202, 4A-203 & cmt. (1998). Section 4A-202 solves this problem for a bank and its customer who has agreed to transact its banking electronically and to be subject to Article 4A. *Id.* If the bank verifies the payment order by using a commercially reasonable security procedure, the customer will be bound even if it did not in fact authorize the payment order. § 4A-202(b). If, however, the customer can prove that the person sending the fraudulent payment order did not obtain the information necessary to send such an order from an agent or a source controlled by the customer, the loss is shifted back to the bank. § 4A-203(a)(2). If the bank does not follow the security procedure and the order is fraudulent, the bank generally must cover the loss. § 4A-202(a).

tain records of all relevant communications pertaining to the transaction and keep those records in such a way that the party can show that the records are authentic. For example, if one party to a contract later disputes the nature of its obligations, the other party may need to prove the terms of the contract to a court. A court, however, will first require that the party establish the authenticity of the record that the party retained of that communication before the court will consider it as evidence.[77]

b. Integrity

Integrity is concerned with the accuracy and completeness of the communication. Is the document the recipient received the same as the document that the sender sent? Is it complete? Has the document been altered either in transmission or storage?

The recipient of an electronic message must be confident of a communication's integrity before the recipient relies and acts on the message. Integrity is critical to e-commerce when it comes to the negotiation and formation of contracts online, the licensing of digital content, and the making of electronic payments, as well as to proving up these transactions using electronic records at a later date. For example, consider the case of a building contractor who wants to solicit bids from subcontractors and submit its proposal to the government online. The building contractor must be able to verify that the messages containing the bids upon which it will rely in formulating its proposal have not been altered. Likewise, if the contractor ever needs to prove the amount of the subcontractor's bid, a court will first require that the contractor establish the integrity of the record he retained of that communication before the court will consider it as evidence in the case.[78]

c. Nonrepudiation

Nonrepudiation is the ability to hold the sender to his communication in the event of a dispute.[79] A party's willingness to rely on a communication, contract, or funds transfer request is contingent upon having some level of comfort that the party can prevent the sender from denying that he sent the communication (if, in fact, he did send it), or claim that the contents of the communication as received are not the same as what the sender sent (if, in fact, they are what was sent). For

77. *See, e.g.*, U.S. v. Eisenberg, 807 F.2d 1446 (8th Cir. 1986) (disputing the authenticity of letter); U.S. v. Grande, 620 F.2d 1026 (4th Cir. 1980) (disputing authenticity of invoice), *cert. denied*, 449 U.S. 830, 919 (1980).

78. *See, e.g.*, Victory Med. Hosp. v. Rice, 493 N.E.2d 117 (Ill. App. Ct. 1986).

79. *See Digital Signature Guidelines*, *supra* note 8. One definition of nonrepudiation is "[s]trong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents." *Id.* § 120.

example, a stockbroker who accepts buy/sell orders over the Internet would not want his client to be able to place an order for a volatile commodity, such as a pork bellies futures contract, and then be able to confirm the order if the market goes up and repudiate the order if the market goes south.[80]

With paper-based transactions, a party can rely on numerous indicators of trust to determine whether the signature is authentic and the document has not been altered. These include using paper (sometimes with watermarks, colored backgrounds, or other indicia of reliability) to which the message is affixed and not easily altered, letterhead, handwritten ink signatures, sealed envelopes for delivery via a trusted third party (such as the U.S. Postal Service), personal contact between the parties, and the like. With electronic communications, however, none of these indicators of trust are present. All that can be communicated are bits (0s and 1s) that are in all respects identical and can be easily copied and modified.

This has two important consequences. First, it often becomes extremely difficult to know when one can rely on the integrity and authenticity of an electronic message. This, of course, makes difficult those decisions that involve entering into contracts, shipping products, making payments, or otherwise changing one's position in reliance on an electronic message. Second, this lack of reliability makes proving up one's case in court virtually impossible. For example, while a typewritten name appended at the end of an e-mail message may qualify as a signature under applicable law, that name could have been typed by anyone, and if the defendant denies the "signature" in a lawsuit, it may be virtually impossible for the plaintiff to prove the authenticity of that signature. As a result, nonrepudiation is by no means assured in such a case, and parties thus may choose to forego e-commerce where the risk of repudiation is too great.

In many respects, trust is a key element of the measurement of risk. And the need for trust can vary significantly, depending on the risk involved. Selling books on the Internet, for example, may not require a high level of trust in each transaction, especially where a credit card number is provided and the risk of loss from fraud is relatively low (e.g., a $20 book). On the other hand, entering into long-term, high-dollar value contracts electronically may require a much higher level of trust. At a minimum, the risk of a fraudulent message must be acceptable given the nature and size of the transaction.

Thus, where the amount at issue is relatively small or the risk is otherwise low, trust in an electronic message's authenticity and integrity

80. *See generally Follow the Money—A New Stock Market Arises on the Internet*, SCI. AM. 31 (July 1995).

may not be a critical issue. If e-commerce is to reach its full potential, however, parties must be able to trust electronic communications for a wide range of transactions, particularly ones where the size of the transaction is substantial or the nature of the transaction is of higher risk. In such cases, a party relying on an electronic communication will need to know, at the time of reliance, whether the message is authentic, whether the integrity of its contents is intact, and, equally important, whether the relying party can establish both of those facts in court if a dispute arises (i.e., nonrepudiation).

2. *The Legislative Response*

Most electronic signature statutes simply do not address the issue of trust at all. Those statutes that do focus on the issue take two different approaches, although either approach requires implementation of rules or standards, or a procedure or mechanism, for determining which technologies are capable of creating such trustworthy signatures, and when, and under what circumstances, that capability is considered fulfilled.

Under the first approach, a trustworthy electronic signature is a precondition to enforceability as a signature. Statutes adopting this approach typically require that electronic signatures possess four attributes—i.e., the electronic signature must be: (1) unique to the person using it; (2) capable of verification; (3) under the sole control of the person using it; and (4) linked to the data in such a manner that if the data is changed, the signature is invalidated.[81] If all of these requirements are met, the electronic signature will be deemed to be a signature for purposes of that state's various statutory and regulatory signature requirements—i.e., the electronic signature will be enforceable.

A number of other statutes have adopted a second approach. These statutes state that almost any form of electronic signature can be enforceable and meet legal signature requirements, while recognizing that some electronic signatures are more trustworthy than others.[82] To encourage the use of those electronic signatures deemed to be more trustworthy, and to provide relying parties with an enhanced level of assurance at the time of reliance regarding the authenticity and integrity of messages using such signatures, these statutes typically provide a legal benefit in the form of an evidentiary presumption regarding the

81. *See generally supra* note 62 (providing a list of statutes adopting this approach).

82. Electronic signatures, like traditional signatures of ink on paper, come in varying degrees of security. A handwritten signature, for example, is more trustworthy than an "X," and a notarized signature is more trustworthy than both. Just as the law provides certain benefits to the more trustworthy forms (e.g., notarized signatures are considered self-authenticating by the FEDERAL RULES OF EVIDENCE 902(8)), these electronic signature statutes seek to define the characteristics required for a trustworthy (or secure) signature.

sender's identity and/or the integrity of the document.[83] Yet, the criteria for determining which technologies and which messages are sufficiently trustworthy to be accorded the benefit of such legal presumptions have varied significantly from statute to statute.

Some of these statutes take a technology-neutral approach to identifying the class of trustworthy electronic signatures that qualify for such a legal benefit. For example, the Illinois Electronic Commerce Security Act creates a class of trustworthy signatures called "secure electronic signatures."[84] In addition to certain requirements regarding implementation,[85] a signature qualifies as "secure" if the parties to the transaction agree on such a characterization, or if the technology used to create the signature is certified by the Secretary of State as capable of creating, in a trustworthy manner, an electronic signature that:

- [i]s unique to the signer within the context in which it is used;
- can be used to objectively identify the person signing the electronic record;
- was reliably created by such identified person;

---

83. Courts have recognized that the legislature has the authority to establish legal presumptions. For Illinois examples, see People v. Rolfingsmeyer, 461 N.E.2d 410, 412 (Ill. 1984) ("[I]t is clear that the legislature of a state has the power to prescribe new and alter existing rules of evidence or to prescribe methods of proof."); Heitz v. Hogan, 480 N.E.2d 185, 189 (Ill. App. Ct. 1985). Moreover, numerous Illinois statutes provide for a variety of different evidentiary presumptions. *See, e.g.,*, 35 ILL. COMP. STAT. 5/503 (West 1998) ("The fact that an individual's name is signed to a return or notice shall be prima facie evidence for all purposes that such document was actually signed by such individual."); 10 ILL. COMP. STAT. 5/10-10 (West 1998). The statute states that:

> In the event of a State Electoral Board hearing on objections to a petition for an amendment to Article IV of the Constitution . . . , or to a petition for a question of public policy to be submitted to the voters of the entire state, the certificates of the county clerks and boards of election commissioners showing the results of the random sample of signatures on the petition shall be prima facie valid and accurate, and shall be presumed to establish the number of valid and invalid signatures on the petition sheets reviewed in the random sample . . . .

Id; 750 ILL. COMP. STAT. 45/5 (West 1998) (providing that a man is presumed to be the natural father of a child if certain conditions are met, and providing further that such presumption "may be rebutted only by clear and convincing evidence"); 720 ILL. COMP. STAT. 5/16-11 (West 1998) (stating that possession of a device that intercepts or decodes the transmission of cable television service is prima facie evidence of a violation of this section prohibiting the unauthorized use of a television interception or decoding device); 725 ILL. COMP. STAT. 150/7 (West 1998) (specifying situations that give rise to a presumption that certain property was furnished in exchange for a substance in violation of the Illinois Controlled Substances Act, which presumptions are "rebuttable by a preponderance of the evidence").

84. 5 ILL. COMP. STAT. 175/1-110 (effective July1, 1999). This Act also defines a class of secure electronic records. *Id.* at 175/10-110.

85. *See* 5 ILL. COMP. STAT. 175/10-110(a). The electronic signature must be (1) created in a manner that was commercially reasonable under the circumstances; (2) applied by the relying party (to verify the signature) in a trustworthy manner; and (3) reasonably and in good faith relied upon by the relying party. *Id.*

• and[86] is created and is linked to the electronic record to which it relates in a manner such that if the record or the signature is intentionally or unintentionally changed after signing the electronic signature is invalidated.[87]

An electronic signature that qualifies as a secure electronic signature enjoys a rebuttable presumption that the signature is that of the person to whom it correlates.[88] Similar types of presumptions for a technology-neutral class of secure records and secure signatures appear in legislation that has been enacted in South Carolina and Singapore.[89] Other technology-neutral electronic signature legislation incorporating rebuttable presumptions (although limited to certain types of transactions) has been enacted in Alabama (limited to certain tax-related usage)[90] and in Ohio (limited to certain health care usage).[91]

Technology-specific statutes that confer similar legal presumptions have been enacted in Minnesota, Missouri, Utah, and Washington, and all such statutes focus solely on digital signature technology.[92] To ensure that the digital signature possesses a level of trust sufficient to warrant enhanced legal recognition, these statutes impose a regulatory structure on certification authorities who voluntarily elect to be licensed

86. *Id.* For example, an electronic signature might be reliably created by a specific person if some aspect of the procedure used to create the signature involves the use of a signature device or other means or method that is under the sole control of such person.

87. *Id.* Note that these four requirements, while similar to the four requirements imposed by the statutes in the second category noted above, are also different in two significant ways. *Id.* First, satisfaction of these requirements is *not* a precondition to creating an enforceable signature, but rather is only a precondition to qualifying as a secure signature entitled to an additional legal benefit of an evidentiary presumption. *Id.* Second, the requirements themselves differ. *Id.* Relative uniqueness, rather than absolute uniqueness, is all that is required for the first element. *Id.* The second element focuses on objective identification, rather than focusing merely on being "capable of verification." *Id.* The third element rejects the "sole control" requirement and focuses instead on a reliable assurance that the named signer actually signed or authorized the signature. *Id.*

88. 5 ILL. COMP. STAT. 175/10-120 (effective July 1, 1999).

89. The concepts of a "secure electronic record" and a "secure electronic signature" were first introduced in the October 14, 1997 draft of the Illinois Electronic Commerce Security Act released for public comment by the Illinois Commission on Electronic Commerce and Crime (copy on file with authors). That concept was subsequently incorporated in the final enacted version of the Illinois Electronic Commerce Security Act, as well as in legislation enacted in South Carolina and Singapore. It has also been used in the draft legislation being considered by UNCITRAL (which renamed the concept "enhanced electronic signature"). *See* 5 ILL. COMP. STAT. 175; S.C. CODE. § 26-5-330 (Law Co-op. 1998); UNCITRAL, *Draft Articles on Electronic Signatures* (December 15, 1998) <http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-80.htm>; *Singapore Electronic Transactions Act*, *supra* note 32.

90. ALA. CODE § 40-30-5 (1999).

91. OHIO REV. CODE ANN. § 3701.75 (West 1999).

92. *See* MINN. STAT. ANN. § 325K.20 (West 1998); MO. ANN. STAT. § 28.677 (West 1998); UTAH CODE ANN. §46-3-101 (1998); WASH. REV. CODE.§ 19/34/900 (West 1998).

by the State.[93] Based on the apparent assumption that all certificates issued by licensed certification authorities are trustworthy, and that a digital signature that is created using the private key corresponding to the public key listed in such a certificate is a trustworthy signature, the legislation has bestowed attributes of trust to messages verifiable by such certificates.[94]

3. *The Role of Legislation in Promoting Trust*

Whether electronic signature legislation should address the issue of trust, and, if so, whether such legislation should require some level of trust as a precondition to enforceability, or offer the benefit of trust (in the form of evidentiary presumptions) as an incentive to use more secure signature methods, is an issue that has generated rather extensive controversy.

Evidentiary presumptions serve a variety of purposes:

> One purpose is to allocate the burden of production or persuasion to the party in the better position to have the evidence. The common law presumption that a letter reaches its addressee if it is properly addressed, stamped, and deposited in the U.S. mail serves such a purpose. Obviously, the sender usually will be in no position to prove receipt. Only the addressee can affirmatively prove receipt or testify that he did not receive the letter. A second purpose of evidentiary presumptions is 'to avoid an impasse, to reach some result, even though it is an arbitrary one.' . . . Finally, most presumptions coincide with what is probably true. For example, the husband of the mother usually is the father of the child.[95]

For electronic transactions, presumptions of the signer's identity and of message integrity can help to provide necessary assurances to relying parties, thereby enabling them to engage in online commercial activities with confidence that their transactions will be easier to enforce in court if that should be necessary. Such presumptions can provide the predictability and trust necessary to rely on a message, and act accord-

---

93. *See, e.g.*, MINN. STAT. ANN. § 325K.20; MO. ANN. STAT. § 28.677; UTAH CODE ANN. § 46-3-101; WASH. REV. CODE § 19/34/100. The digital signature legislation enacted in Germany, Italy, and Malaysia contains a similar approach.

94. *See, e.g.*, UTAH CODE ANN. § 406(3). The Utah Digital Signature Act provides that if a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority, then a court of the State of Utah "shall presume that": (a) the digital signature is the digital signature of the subscriber listed in that certificate, and (b) the digital signature was affixed by that subscriber with the intention of signing the message. *Id.*

95. Keith B. Hall, *Practitioner's Note: Evidentiary Presumptions*, 72 TUL. L. REV. 1321, at 1325-26 (Mar. 1998) (quoting from MCCORMICK ON EVIDENCE § 343 (4th Ed. 1992)).

ingly, in real time.[96] Such presumptions are based on the trustworthiness of the security procedure used to create the electronic signature, and the fact that the purported sender is more likely than the recipient to possess the information necessary to prove or disprove the validity of the signature.

Yet the use of presumptions in electronic signature legislation has also been criticized.[97] Such criticism has centered on concerns that consumers and small businesses that lack an understanding of the sophisticated technologies used to create the secure electronic signature may unwittingly find themselves in a situation where their failure to protect the security of their signature device (e.g., their private key) will expose them to substantial liability for unauthorized transactions made by persons who unlawfully obtained access to their signature device.[98] Unfortunately, the debate on either side of the issue has not rigorously analyzed the attendant legal and policy issues involved, and often has focused solely on emotional arguments such as "grandma could lose her private key and someone could sell her house and clean out her bank account."

The criticism has also been particularly vocal regarding technology-specific statutes that impose highly regulatory schemes and licensing requirements in exchange for presumptions. Beyond the obvious problems that can be anticipated by the prospect of fifty different state licensing schemes as well as a separate (and presumably incompatible) licensing scheme that varies from country to country, these technology-specific statutes are problematic because they appear to assume that only digital signature technology is worthy of trust, assume or even require the use

96. A related issue is the effect of the presumption. Several statutes also give different effects to presumptions. In some cases, the presumption is merely a prima facie case. *See, e.g.*, 35 ILL. COMP. STAT. 5/503 (West 1998). In other cases, the statute defines the presumption in terms of the burden of going forward with the evidence. *See, e.g.*, 740 ILL. COMP. STAT. 95/4 (West 1998) (noting that "[t]he presumption provided shall only shift to the defendant the burden of going forward with evidence, and shall in no event shift the burden of proof to the defendant"). In still other cases, the presumption is rebutted by a preponderance of the evidence. *See, e.g.*, 725 ILL. COMP. STAT. 150/7 (West 1998) (referring to "such presumptions being rebutted by a preponderance of the evidence"). Current law also provides that "a signature on a document filed by facsimile in accordance with rules adopted by the Secretary of State is prima facie evidence for all purposes that the document actually was signed by the person whose signature appears on the facsimile." 15 ILL. COMP. STAT. 305/15 (West 1998).

97. Early drafts of the Uniform Electronic Transactions Act, for example, included presumptions similar to those in the Illinois Electronic Commerce Security Act, but the drafting committee ultimately voted to remove all presumptions from the UETA.

98. *See also* Reporter to the Uniform Electronic Transactions Act Drafting Committee, *Memorandum* (Sept. 18, 1998 draft) <http://www.law.upenn.edu/library/ulc/uecicta/eta1098m.html> (discussing some of the reasons favoring and disfavoring the use of presumptions in electronic signature legislation).

of a particular business model for the implementation of digital signatures, and require a relatively high (and therefore costly) level of authentication by the certification authority in order to ensure that the certificates are trustworthy. Critics say that the net result, on a global basis, may very well be the inhibition of e-commerce by virtue of incompatibilities between jurisdictions, the erection of potential trade barriers between jurisdictions, and the imposition of significant costs and operational constraints upon certification authorities and trading partners engaged in electronic transactions. In other words, in taking one step forward, we may be taking two steps back.

Whether legislation should address the issue of trust for e-commerce, and whether it should do so in the form of presumptions or through some other means, is an issue that deserves thorough study and analysis. Suffice it to say, for purposes of this article, that developing practical and workable legislative approaches to the issue of trust in e-commerce could be critical to the growth of business-to-business and, ultimately, business-to-consumer transactions.

C. WHAT ARE THE RULES OF CONDUCT?

1. *The Issue*

In addition to facilitating the trust necessary to encourage users of e-commerce messages to act in reliance on them, electronic signature legislation can provide the predictability required by businesses to engage in e-commerce transactions. Predictability is a watchword for the growth of commerce, and law can play a key role in providing this valuable commodity.[99]

---

99. Numerous commentators have discussed the need for predictability and the role played by the law in providing such predictability. For example, in discussing the growth of the lumber industry in Wisconsin in the 1800s, legal scholar James Willard Hurst noted that "[b]ecause marketing cannot go on save in a context of reasonably assured expectations, the legal order as a whole was, of course, indispensable to the existence of a market." JAMES WILLARD HURST, LAW AND ECONOMIC GROWTH: THE LEGAL HISTORY OF THE LUMBER INDUSTRY IN WISCONSIN 1836-1915 285 (1964) [hereinafter LAW AND ECONOMIC GROWTH]. Legal scholar Lawrence M. Friedman, in discussing American common law's move away from formality for its own sake over the past two centuries, emphasized that the businessman had no need for "ceremonial formalism" but rather valued "substantive predictability"—"[e]conomic decisions depended upon the ability to know, within limits, what was 'the law.'" LAWRENCE M. FRIEDMAN, CONTRACT LAW IN AMERICA: A SOCIAL AND ECONOMIC CASE STUDY 92 (1965) [hereinafter CONTRACT LAW IN AMERICA]. Oliver Wendell Holmes, Jr., one of this country's greatest jurists, observed that:

> People want to know under what circumstances and how far they will run the risk of coming against what is so much stronger than themselves, and hence it becomes a business to find out when this danger is to be feared. The object of our study, then, is prediction, the prediction of the incidence of the public force through the instrumentality of the courts.

Predictability in e-commerce will no doubt be founded upon many sources of relevant law: longstanding principles of freedom of contract in which parties determine the terms that will govern their online transactions, the rich common law tradition of judge-made precedent recognizing such contracting principles and shedding light on statutes governing commercial transactions, and legislation geared to e-commerce as well as statutes of more general application. For example, as James Willard Hurst noted in his analysis of the legal history of the lumber industry in Wisconsin between 1836 and 1915, the relevant law for providing the reasonably assured expectations that were essential to the growth of the industry included not only that of simple contracts, but also "the law of more complex arrangements of negotiable instruments, of secured transactions (mortgage, pledge, reserved title, lien), of business association (joint venture, partnership, corporation), and of insurance."[100]

The difficult question is how predictability can best be provided to advance e-commerce. The Internet is revolutionizing the way that companies do business, and parties engaging in online transactions face novel legal challenges that test the limits of existing statutory and case law. In many instances, the rules in e-commerce transactions will follow from the rules set forth for paper-based transactions. For example, to be enforceable, certain contracts must be signed by the party to be bound. Likewise, for a contract to be valid, there must be an offer and acceptance as well as consideration for the transaction. In other instances, however, e-commerce transactions have raised, and will continue to raise, issues not easily answered by extensions of traditional law, particularly regarding issues that are unique to a specific technology.

For example, while electronic signatures created through the use of a digitized handwritten signature (or even via signature dynamics) are probably governed by traditional rules relating to signatures, electronic signatures created through the use of digital signatures raise a host of new legal issues. Because digital signatures are created by using a unique and secret private key that is associated with the signer, an issue is raised as to the liability of the identified signer if the private key is compromised and the signature is, in fact, created by someone else. Likewise, because digital signatures frequently involve the use of certificates to establish identity, and because certificates are typically issued by a trusted third party, issues are raised as to the obligations of that

---

RICHARD A. POSNER, THE ESSENTIAL HOLMES 160 (1992) (citing Oliver Wendell Holmes, Jr., *The Path of the Law*, 10 HARV. L. REV. 457 (1897)). As U.C.C. Art. 2 drafter and legal scholar Karl Llewellyn noted in his treatise on jurisprudence, the true ideal is not really certainty but rather "reasonable regularity of decision" or "a reckonability equivalent to that of a good business risk." KARL N. LLEWELLYN, THE COMMON LAW TRADITION: DECIDING APPEALS 216, 18 (1960).

100. *See* LAW AND ECONOMIC GROWTH, *supra* note 99, at 285.

third party and its potential liability in the event that certificates are erroneously issued, improperly verified, or not revoked upon request.

2. *The Legislative Response*

Most electronic signature statutes enacted to date say nothing about the rules governing the conduct of parties using electronic signatures. A few states have, however, enacted legislation addressing at least some of the rules governing the conduct of the parties. This legislation generally falls into two categories.

The first category is exemplified by the technology-specific digital signature legislation enacted in Minnesota, Missouri, Utah, and Washington.[101] These statutes address a variety of issues raised by the use of public key technology. First, they specify the scope of the obligations of the person obtaining a digital certificate to:

- make truthful representations in applying for a certificate;
- review and accept a certificate before using it;
- make certain representations upon acceptance of the certificate;
- control and keep confidential the person's private key;
- and promptly revoke the certificate upon compromise of the underlying private key.

Such statutes also extensively outline the obligations of certification authorities outline the obligations that seek the benefit of the state licensing provisions (and, in some cases, of all certification authorities, whether or not licensed). Typically specify the obligations of the certification authority to:

- use a trustworthy system;
- disclose its practices and procedures;
- properly identify a prospective applicant for a certificate;
- publish issued certificates in a repository;
- suspend and/or revoke certificates;
- make warranties to the certificate applicant upon issuance of the certificate; and
- make warranties to persons using the certificate to verify digitally signed messages.

These statutes also usually specify qualifications required to become a licensed certification authority, including rules governing personnel, the filing of a bond or suitable guaranty, the use of a trustworthy system, the possession of sufficient working capital, the maintenance of an office in the state, and the compliance with other licensing requirements established by the state.[102] The statutes also permit certification authorities to limit their liability in a variety of ways.

101. *See generally supra* note 93.

102. *See supra* note 93.

Some technology-neutral electronic signature statutes address issues related to the general use of electronic signatures, including rules regarding:

- the creation and control of signature devices used by the signers of electronic messages to produce a unique electronic signature;
- instances in which signatures would be attributed to the named signer;
- the unauthorized use of signature devices;
- whether a party is obligated to accept an electronic signature; and
- the circumstances under which the parties to a transaction may vary the provisions of the statute (i.e., party autonomy).[103]

In some cases, such as those involving the licensing of certification authorities, the statute establishes a regulatory structure. In other cases, however, the statutory rules simply address questions bound to arise sooner or later. For example, if a private key is compromised, and an unauthorized message is used to defraud an unsuspecting third party, we must answer the question of which party (i.e., the defrauded third party or the person whose signature was "forged") should bear the resulting loss. Although numerous public policy arguments can be made for each position, the fact remains that different questions such as these cannot be indefinitely ignored—if they are not addressed by a contract between the parties, they must either be answered legislatively or, if all else fails, by a court.

Most forms of electronic signature legislation that apply to business-to-business transactions provide few if any, provisions relating to the rules governing the conduct of the parties using electronic signatures. Many statutes simply specify the attributes required before an electronic signature will be considered enforceable. Several do, however, provide that the use or acceptance of an electronic signature is at the option of the parties to the transaction.[104] A few other statutes also provide some limited rules governing the conduct of the parties using electronic signatures. These include, for example, Georgia, which provides a remedy for a person whose electronic signature is used in an unauthorized fashion;[105] Hawaii, which provides that a time-stamp is prima facie evidence that the time-stamped signature took effect as of the date and time indicated in the time-stamp;[106] and Illinois, which provides rules relating to electronic recordkeeping, the creation and control of signature devices,

103. *See, e.g.*, 5 ILL. COMP. STAT. 175 (effective July 1, 1999); *see also* Uniform Computer Information Transactions Act (Feb. 1, 1999 draft).

104. *See, e.g.*, CAL. GOV'T CODE § 16.5 (West 1999); GA. CODE ANN. § 10-12-4 (Michie 1998); 5 ILL. COMP. STAT. 175/5-140; N.H. REV. STAT. ANN. § 294-D:4 (1999); OKLA. STAT. ANN. tit. 15 § 965 (West 1999); S.C. CODE ANN. § 26-5-330 (Law. Co-op. 1998); W. VA. CODE § 39-5-2(e) (1998).

105. GA. CODE ANN. § 10-12-4.

106. HAW. REV. STAT. ANN. § 231-8-5 (Michie 1998).

and the rights and responsibilities of parties using digital signatures.[107]

A key issue that arises when prescribing rules of conduct for the parties is whether such rules should be mandatory or operate simply as gap-fillers (i.e., default rules that can be varied by contract). This issue of party autonomy (i.e., freedom of contract) has also been critical for the United States in the context of its international negotiations regarding electronic signatures through the UNCITRAL Working Group on Electronic Commerce. However, those seeking a regulatory licensing regime governing certification authority services and the use of digital signatures, and persons seeking strong consumer protection, have all favored legislation containing certain provisions that cannot be varied by an agreement of the parties.

A review of existing U.S. electronic signature legislation reveals very few statutes that address these issues. The technology-specific digital signature statutes enacted in Minnesota, Missouri, Utah, and Washington, which provide for the voluntary licensing of certification authorities, all contain numerous provisions that cannot be varied by agreement of the parties. Moreover, they do not contain a general party autonomy provision. Conversely, the electronic signature legislation enacted in Illinois, as well as the proposed Uniform Electronic Transactions Act, contain express provisions authorizing parties to a transaction to vary the terms of the statute by agreement between them. Most other legislation is simply silent on the subject of party autonomy. This includes the legislation specifying the four conditions of trust that must be present before an electronic signature will be considered enforceable, thereby leaving unanswered the question of whether the contracting parties may agree between themselves to accept an electronic signature that does not meet the requirements of those statutes.

3. *The Role of Legislation in Specifying the Rules of Conduct*

a. The Need for Predictability

As we indicated earlier, most electronic signature statutes do not go beyond the basic question of affirming that e-commerce transactions are in fact enforceable. Yet, we should not discount the predictive value that legislation could provide to contracting parties, particularly where the technological issues are complex. Although courts typically strive to achieve reckonability of result and to reflect prevailing commercial practices in the opinions they issue, and the Uniform Commercial Code is designed to permit courts to develop the law of commercial transactions "in the light of unforeseen and new circumstances and practices,"[108]

107. *See* 5 ILL. COMP. STAT. 175/5-105 (effective July 1, 1999).

108. U.C.C. § 1-102, cmt. 1 (1998).

many judges will likely feel hard pressed to grapple with some of the unique issues raised by the rapid and complex technological changes associated with e-commerce.

For example, while most courts would probably feel comfortable in extending the law to hold that electronic transactions are legal, can the same be said about the host of new and highly technical legal issues raised by the use of digital signatures? An electronic signature statute that merely indicates that electronic transactions are enforceable does nothing to resolve the issue of liability of an identified signer when a private key has been compromised, or of a certification authority for erroneously issuing or improperly verifying digital certificates. Lacking well-built rules fashioned by the legislature to address such complexities, will the decisions that are issued by courts be perceived to be the right ones? Given the novelty of the legal issues, what will be the cost to predictability, and thus the nationwide growth of e-commerce, of conflicting (albeit well-reasoned) court opinions that vary from jurisdiction to jurisdiction and, perhaps, from judge to judge?

Although a believer in the Grand Style of judging, Karl Llewellyn—the central figure in drafting Article 2 of the Uniform Commercial Code (the latter of which has been described as the most successful codification of American law)—emphasized that judges must be given the proper tools in the form of rules well-built to fit the situation. He advocated "'the on-going production and improvement of rules which make sense on their face, and which can be understood and reasonably well applied even by mediocre men.'"[109] Llewellyn attacked the then-current sales law as being "full of rules and concepts that are badly tailored to the facts and needs of life, full therefore of situations in which it takes a better than average judge to get results which are both sound in result and clean in doctrinal craftsmanship and clear guidance for the future."[110]

Although courts will no doubt strive for continuity and predictability of result in their opinions, we should consider the alternative to a case-by-case, wait-and-see revelation of the law of e-commerce. As Llewellyn observed:

---

109. Zipporah Batshaw Wiseman, *The Limits of Vision: Karl Llewellyn and the Merchant Rules,* 100 HARV. L. REV. 465, 494 (Jan. 1987) (citing KARL N. LLEWELLYN, *supra* note 99, at 38).

110. Wiseman, *supra* note 109 (citing Karl N. Llewellyn in an undated paper, apparently written between 1943 and 1949). In Llewellyn's treatise in which he discussed the need for predictability and reckonability in jurisprudence, which sheds light on the need for specificity in the drafting of legislation, Llewellyn similarly noted that ". . . probability in prediction will vary with the technical excellence of the rule itself—i.e., of its tailoring to purpose. . . ." KARL N. LLEWELLYN, THE COMMON LAW TRADITION: DECIDING APPEALS 181 (1960).

> [w]hat does it cost a polity in delay and uncertainty and in legal discomfort or injustice to have the making or review of a rule wait upon the chance raising and appeal of issues one by one by dragging one? Consider, in contrast, what a Uniform Commercial Act or a Uniform Commercial Code does in making available in a jurisdiction where rulings are sparse the experience and wisdom of the whole country—all at a single stroke. Or consider the problem of accessibility of doctrine as it bears on the man-hours of talented labor (if there is to be accuracy based on knowledge), and so on the expense, needed for advice.[111]

If properly drafted, statutes arguably can provide greater certainty and predictability in a shorter period of time. The question arises whether the "slow drip, drip of case-law wearing away the stony abstraction of the law"[112] is the best way to promote e-commerce and develop the legal guideposts by which companies steer their course. Unlike courts, which as *interpreters* of the law must wait until a dispute arises before they can in effect *make* law regarding a particular statute or issue, state and federal legislatures are continually poised to create new laws and amend or abolish existing laws. While legislatures can systematically approach a given set of issues and troubleshoot areas of perceived legal uncertainty for contracting parties, courts must limit themselves to actual disputes: "[i]t is no answer to say that all important questions will turn into disputes; 'disputes' are not litigation, and only litigation—primarily, appellate litigation—makes new law. . . . The common law is therefore not only slow; it is impotent to effect certain kinds of significant legal change."[113]

Likewise, it is no answer to say that private parties can merely contract around any areas of legal uncertainty. The world has embraced e-commerce in many respects because of the potential it offers for reducing transaction costs, increasing efficiency, and streamlining transactions. Requiring parties to contract around areas of legal uncertainty while waiting months and even years for needed precedent from the courts might actually increase transaction costs, decrease efficiency, and impose cumbersome contracting obligations that would not be necessary in more traditional paper-based transactions. Therefore, we should not discount the potential value offered by legislation that establishes default rules regarding electronic signatures and other related e-commerce issues. Such default rules can lower transaction costs because the parties need not try to spell out or anticipate every possible scenario arising out

111. *See* LLEWELLYN, *supra* note 99, at 518. *See also* U.S. Government, *Framework for Global Electronic Commerce* (visited Sept. 18, 1998) <http://www.ecommerce.gov/framewrk.htm> ("To encourage electronic commerce, the U.S. government should support the development of both a domestic and global uniform commercial legal framework that recognizes, facilitates, and enforces electronic transactions worldwide.").

112. CONTRACT LAW IN AMERICA, *supra* note 99, at 245.

113. LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 22 (2d ed. 1985).

of the transaction.[114] Nor should we assume that parties will always resolve all issues relating to electronic signatures through their agreements. Most commercial transactions, especially those that become relatively routine, are characterized by shorter and shorter agreements that frequently fail to deal with many of the issues that could arise.

While such cost concerns are likely to be important for all parties doing business online, they can be key for entrepreneurs launching their businesses on the Internet; for some of these start-ups, legal fees are an expense that they cannot afford,[115] and yet entering into contracts in which the legal consequences are not clear also poses a risk where the price may be too high. Instead, electronic signature legislation can provide rules that show parties how they can minimize risk regarding new technologies (i.e., digital signatures), and prevent disputes from occurring in the first place, by determining in advance what consequences will follow from certain action. Avoiding disputes is a desirable objective from a business point of view; in addition to the legal costs involved, litigation can be expensive in terms of damaged business relationships, adverse publicity, and loss of good will.

Providing predictability in business transactions through legislation might well include specifying the rules governing the conduct of the parties and, as a consequence, defining the risks and liabilities of the parties to the transaction. We should consider whether taking a legislative approach to developing the law of e-commerce would have any advantages over relying solely on a case-by-case approach. An ounce of prevention through the legislative establishment of default rules could well be worth a pound of cure.

b. The Proper Role of Technology Neutrality

The U.S. government and numerous commentators have stressed that e-commerce legislation should be "technology neutral." In fact, in many circles, this has become the mantra by which electronic signature legislation is evaluated. According to the *Framework for Global Electronic Commerce,* for example, "rules should be technology-neutral (i.e.,

114. Indeed, it seems particularly fitting that "default rules" should be established to govern the computer-driven world of e-commerce, given that the term "default rules" is computer jargon for rules that a computer program automatically follows unless the user specifies otherwise.

115. While lawyers will no doubt be called upon to interpret the statutes that are enacted, a dispute with a trading partner over a murky digital signature issue (especially a dispute that may well have to climb its way to the appellate level against a well-financed litigant) could be far more cost-prohibitive and more likely to thwart the growth of e-commerce.

the rules should neither require nor assume a particular technology)."[116] Similarly, the U.S. proposal for an international convention on e-commerce states as follows:

> Technology Neutrality—Any rules should neither require nor hinder the use or development of authentication technologies. States should anticipate that authentication methods will change over time and avoid legislation that might preclude innovation or new applications. States should avoid laws that intentionally or unintentionally drive the private sector to adopt only one particular technology for electronic authentication to the exclusion of other viable authentication methods.[117]

This position grows, in part, out of the concern that legislation addressing one particular form of electronic authentication (e.g., digital signatures) may have the unintended consequence of precluding other methods of authentication that might also be appropriate, and thus inhibit the development of other technologies that might be equal or superior to digital signatures. In other words, states and countries should recognize that there are (or will be) many methods that will be sufficiently reliable for authenticating electronic messages for a given purpose.

Yet what is meant by the term "technology neutral" is often not clear. In some cases it is a code for the position that legislation should not address the special issues raised by any specific technology. In other cases, it means that legislation should not unfairly favor one technology over another. These are, however, two different positions, as the latter view does not necessarily prohibit a legislative solution to the new issues raised by one technology (such as digital signatures), so long as that solution does not discriminate against other similar technologies.

Attaining the ideal of technology neutrality need not preclude consideration of unique and legitimate legal issues raised by the use of a digital signature PKI[118] infrastructure. Quite simply, the use of digital signatures raises a set of singular issues that must be addressed at some point by transacting parties. These issues include the responsibility of the signer of a message for the use or misuse of the signer's private key, the obligation of a certification authority to properly authenticate persons to whom it issues certificates, and the responsibility of message recipients to verify the integrity of the digital signature before relying on it. In a closed PKI system, these issues and others can, of course, be

116. *Framework for Global Electronic Commerce* (July 1, 1997) <http://www.ecommerce.gov/framewrk.htm>.

117. *Draft International Convention on Electronic Transactions* (May 25, 1998 draft) <http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-77.htm>.

118. "PKI" or "public key infrastructure" means the framework of rules governing the rights and responsibilities of participants in a system that uses public key cryptography for purposes of authentication and ensuring integrity and/or of encryption.

addressed by contractual agreement between the parties. But the fact that all fifty states have adopted a rather extensive Uniform Commercial Code designed primarily to provide "gap-filler" provisions suggests that parties engaged in commercial transactions do not always take the time to address every legal issue likely to arise between them.[119] Of course, several commentators have argued that an open PKI system will never develop and that legislation is not needed to address issues raised by such an environment. But this begs the question as to whether it is desirable for an open PKI system to develop and whether legislation providing the needed certainty might facilitate that public policy objective.

Abstract concepts can only go so far in legislation regarding unique technology and communications media. For instance, under First Amendment jurisprudence, broadcasting media (i.e., television and radio) are regulated differently than print media (i.e., newspapers). Broadcasters can be sanctioned for airing indecent speech that would not be sanctioned if it were published in printed form.[120] A number of differences between the various technologies results in such differential regulation. Despite the existence of different statutory schemes for these various technologies and communications industries—whether it be radio, television, cable, telephone, or the like—that has not precluded the development of other new technologies and communications media, such as the Internet. Therefore, creating a statutory scheme that addresses the unique legal issues raised by digital signatures, for example, would not necessarily preclude the development of other such technologies and business models.

As indicated below in our discussion regarding the positive historical role that legislation has played in the economic growth of the U.S., different industries and market segments can raise their own unique legal issues and justify their own particularized statutes. For example, the need to promote growth of the lumber industry in 19th Century Wisconsin led the state legislature to enact log-labor liens to encourage laborers to work in the woods,[121] while the need to encourage construction in early America led state legislatures to establish the mechanic's lien.[122] Likewise, because the promotion of e-commerce has been identified as a desirable public policy goal and because particular types of electronic signatures, such as digital signatures, raise certain unique issues, it may be appropriate to address those issues legislatively so long as it is done in a manner that does not unfairly favor one technology over another.

---

119. Whether gap-filler or default rules should be legislatively resolved only after commercial practice has developed is, of course, an issue that deserves further consideration.

120. F.C.C. v. Pacifica Found., 438 U.S. 726, 748 (1978).

121. *See infra* section C.4.

122. *See infra* section C.4.

4. *Some Closing Thoughts on Why a Legislative Approach May Be Warranted*

We live in an age of statutes[123]—a time when the various state and federal legislatures have emerged as the dominant force in ascertaining public policy and translating it into law.[124] Thus, it is not surprising that forty-nine of the fifty U.S. states have responded legislatively to the legal issues raised by electronic signatures.

It is important to understand, however, that legislation can come in many forms, and produce markedly different results depending on those forms. Statutes, or corresponding regulations, can control or mandate certain behavior as an extension of the state's "police power." Examples abound of instances in which the government has imposed bureaucratic procedures or controls on various industries with the stated purpose of protecting consumers, such as from the dangers of unlicensed occupations,[125] or from railroads that became "overmighty subjects" that had to be controlled by some sort of watchman.[126] It would be hard to dispute that rigid controls or heavy bureaucratic structures imposed on e-commerce in its nascent state could be counterproductive. Likewise, statutes that impose mandatory provisions that parties cannot contract around can seriously inhibit the development of a new industry. Freedom of contract, a guiding principle of the Uniform Commercial Code,[127] should be preserved online, at least in business-to-business transactions.[128] On the other hand, statutes that promote predictability, reduce uncertainty, and provide default rules to fill in gaps in contractual coverage or to minimize the need (and the attendant cost) of contracting to anticipate every possible eventuality can play a facilitating role. These are statutes that are designed not to function as straitjackets that parties cannot contractually get out of, but rather to serve as a welcome guide through unexplored Internet territory.

Good arguments have been made that any electronic signature statute that goes beyond merely removing the most obvious barriers to e-commerce (e.g., going beyond the question of "Is it legal?") will actually

123. ROBERT A. HILLMAN ET AL., COMMON LAW AND EQUITY UNDER THE UNIFORM COMMERCIAL CODE § 1.01, at 1-2 (1985).

124. ABNER J. MIKVA AND ERIC LANE, LEGISLATIVE PROCESS 1 (1993).

125. *See* Friedman, *supra* note 113, at 455-457. Those occupations hearing the "siren song of licensing" saw it as a way to restrict competition and increase the prestige of the trade. *Id.*

126. *Id.* at 449.

127. U.C.C. § 1-102, cmt. 2 (1998).

128. *But see* U.C.C. § 1-102. It is worth remembering that even the U.C.C. contains exceptions to the parties' ability to agree otherwise. *Id.*

hurt, not help, e-commerce.[129] These arguments are especially persuasive when it comes to compulsory controls or regulations that parties cannot contract out of. Although we live in the Information Age, we do not live in a world of perfect information—no crystal ball will tell us whether the electronic signature statute we pass today will in fact achieve its objectives or cause unintended consequences. But we must also keep in mind that doing nothing more than removing the most obvious barriers is not necessarily a "safe" approach to promoting e-commerce and avoiding unintended consequences. It is possible that in standing pat and failing to do what we can do to provide default rules and facilitate trust, we could also be hindering the growth of e-commerce.

Legislation is neither inherently bad nor good. U.S. legal history is filled with examples of statutes that were ill-conceived, ineptly drafted, enacted too early or too late to achieve their objectives, or just simply counterproductive.[130] By the same token, U.S. history also provides numerous instances in which legislation has been extremely beneficial and has functioned to promote, rather than restrict, economic growth.[131]

Legal scholar James Willard Hurst, for example, noted that law was used in Wisconsin as a "positive instrument" to develop the 19th Century lumber industry in that state. Toward that end, the state legislature enacted log-labor liens to encourage laborers to work in the woods, and also included navigation guaranties in stream franchises to expand traffic volume.[132]

Likewise, legal scholar Lawrence M. Friedman has identified numerous instances in which state legislation has been used to facilitate and promote economic growth.[133] Statutes freeing corporations and municipalities from traditional contractual disabilities facilitated economic development and provided a sort of government aid. Legislation also played key roles in ensuring the extension of credit and thus of economic

129. Such arguments include: (1) we do not yet know enough about e-commerce; (2) the time for legislation or regulation is after identifiable problems exist in a mature industry, not before an industry even exists, and (3) drafting commercial statutes that regulate commercial practices that do not exist do not enable commercial transactions but rather impede them.

130. *See generally* JAMES WILLARD HURST, THE GROWTH OF AMERICAN LAW: THE LAW MAKERS (1950); LAW AND ECONOMIC GROWTH, *supra* note 99; CONTRACT LAW IN AMERICA, *supra* note 99; FRIEDMAN *supra* note 113.

131. More often than not, law follows on the heels of change to provide stability and legitimacy: "its role has been much more to organize, channel, legitimize, and in a substantial measure to redirect the course of changes that started outside the law." *See* HURST, *supra* note 130, at 19.

132. *See* LAW AND ECONOMIC GROWTH, *supra* note 99, at 571.

133. *See* FRIEDMAN, *supra* note 113 at 242-246; CONTRACT LAW IN AMERICA, *supra* note 99, at 142-148, 186.

growth in the U.S. For example, "[a] strong mortgage law, giving creditors strong rights, was as necessary for debtors as for creditors, if only to make capital flow into real-estate investment."[134] To lay a foundation for swift development of the economy, state legislatures in many instances also manipulated contract remedies to indirectly encourage such development, such as through the enactment of a variety of lien laws. For example, legislation to create the mechanic's lien was first passed in Maryland to encourage master builders to enter into contracts to erect and finish houses in the new capital city of Washington, D.C.; eventually, state after state adopted increasingly broader versions of the lien, which played a "developmental" role in the growth of the United States, mobilizing labor and capital to ensure that houses got built. Lien laws were "enormously important because of the pervasive, ruinous force of the business cycle. . . . The law reflected a desperate search for security—how to protect one's own assets and how to get recourse against the other man's."[135] Like land grants, mechanic's liens functioned as promotional devices: "[b]y the act of giving real security to the worker, the statute gave a line of credit to the land-owner. . . ."[136]

Without such security, capital may not have flowed as swiftly to develop the new frontier that was the United States. In the early years of America's development, people generally favored:

> legal arrangements which legitimized and encouraged the maximum exercise of private will. But economic growth was the end, rather than some abstract ideal of freedom of private enterprise from public interference. Positive use of law in the economy—land grants to subsidize the building of canals and railroads are a good example—was widely approved where this use of law was deemed likely to promote economic development. Abstraction, then, had to give way whenever it interfered with the greater goal.[137]

The U.S. economy depends more on credit than any other country in the world, and lending institutions in the U.S. are willing to extend credit and transfer funds because of the legal certainty of security interests under U.S. law, specifically Article 9 of the Uniform Commercial Code.[138] Article 9 was designed to apply to "all consensual security interests in personal property and fixtures,"[139] and the aim of the Article

134. *See* FRIEDMAN, *supra* note 113 at 246.

135. *Id.* at 245.

136. *See* CONTRACT LAW IN AMERICA, *supra* note 99, at 43. By the same token, boat and vessel acts (such as the one enacted in Wisconsin in 1838) provided laborers and suppliers with an *in rem* action for claims against vessels in local waters. *Id.* at 144.

137. *Id.* 186.

138. John M. Wilson-Molina, *Mexico's Current Secured Financing System: The Law, the Registries and the Need for Reform* (visited Apr. 10, 1999) <http://www.natlaw.com/pubs/spmxbk3.htm.>.

139. U.C.C. § 9-102, cmt. (1998) (regarding Purposes).

was "to provide a simple and unified structure within which the immense variety of present-day secured financing transactions can go forward with *less cost* and with *greater certainty*."[140] Article 9's success in achieving such objectives, by shaping rules based on commercial lending marketplace principles, "has fostered the development of the world's largest and most active commercial and consumer credit markets."[141]

Conversely, getting credit in Mexico—whose personal property secured financing law has been compared to that of the U.S. before the advent of Article 9[142]—can be difficult and often costs three times more than in the United States or Canada (whose Canadian Personal Property Security Act (PPSA) is based on the U.S. model).[143] Mexico's "crazy quilt" of varying security devices, each with its own filing system and standards for granting priority interests (where it is very difficult to determine whether all the necessary legal documents have been filed to create a binding security agreement), makes filing extremely costly and creates uncertainty, thereby discouraging the extension of credit by banks.[144] As one commentator observed, "Mexican banking laws do not offer the legal certainty and protection demanded by banks needed to given them the confidence to lend money to small start-up companies."[145] The lack of clear investment laws or "rules of the game" thus has hindered Mexico's economic development.[146]

Article 9 provides support for the proposition that codification of legal principles can help reduce costs and increase predictability for contracting parties, thereby promoting economic growth. Yet Article 9 and Mexico's experiences may have even more to teach us about the potential dangers of legislation. Although electronic signature legislation can act as a catalyst in promoting economic growth by increasing predictability, there is a very real danger that a "crazy quilt" of conflicting electronic

---

140. *Id.* § 9-101, cmt. (emphasis added).

141. Dr. Boris Kozolchyk, *What to Do About Mexico's Antiquated Secured Financing Law (Section II.B.)* <http://natlaw.com/pubs/bk9.htm>.

142. *See* Wilson-Molina, *supra* note 138 (citing William H. Hawkland and Alejandro M. Garro, *Committee on Secured Transactions: Introductory Note From the Reporters*, ACADEMIA PUERTORRIQUENA DE JURISPRUDENCIA Y LEGISLACION 3-21 (1989)) ("[E]stablishing that most civil law jurisdictions use a complex system of various personal property secured financing mechanisms to achieve poorer results than those accomplished under UCC Article 9."); DALE B. FURNISH, MEXICAN LAW ON SECURED TRANSACTIONS, IN DOING BUSINESS IN MEXICO 37.01 (SMU ed., 1987).

143. *See* Kozolchyk, *supra* note 141.

144. David W. Eaton, *Transformation of the Maquiladora Industry: The Driving Force Behind the Creation of a NAFTA Regional Economy*, 14 ARIZ. J. INT'L & COMP. LAW 747, 827 (Fall 1997).

145. David W. Eaton, *Mexican Participation in the Maquiladora Industry: Loan Them the Money!!!* 14 ARIZ. J. INT'L & COMP. LAW 329, 332 (Fall 1997).

146. Eaton, *supra* note 144, at 832. Such concerns fueled calls for legislative reform. *See generally supra* notes 142-146.

signature legislation could actually decrease predictability and inhibit the growth of e-commerce.

IV. CONCLUSION

Although it seems proper to reject the imposition of undue restrictions on e-commerce, we must recognize that legislation can, if properly written, encourage rather than restrict, and promote rather than disable, the desirable public policy goal of global e-commerce. In evaluating the merits of electronic signature legislative initiatives, we must be sure to distinguish between regulatory legislation, which often dictates restrictive standards and conditions, and enabling or facilitating legislation, which can be used to support freedom of contract and increase predictability and certainty in online transactions without inhibiting the development of new business models and technology for authentication and message integrity. We must also keep in mind that limiting the legislative helping hand that we extend to e-commerce is not risk-free; benign neglect may well produce stagnation or at least slow the development of business online. Retention of existing law during a period of rapid technological innovation can, paradoxically, create instability and uncertainty. Conversely, when law moves with change in business practice, law can actually have its most stabilizing effect and facilitate economic growth.

We have seen what has already been done by the initial trailblazers in e-commerce—companies whose businesses were already firmly rooted in electronic media (such as the computer industry) or whose businesses translated easily to e-commerce business models.[147] While many are using the Internet to great effect for advertising and distributing other content, many more have yet to realize the ultimate promise of this powerful communications medium to engage in online transactions. The difficult question is this: what role can legislation play in encouraging the exploration of the transactional frontiers that this new world of e-commerce has to offer?

The answers to the legal issues raised in this article are far from clear. Electronic signature legislation can and should serve as a vehicle for advancing e-commerce, but we no doubt will need to adapt our legislative approaches as new business models and technologies emerge and the case law develops. In particular, we should closely monitor whether the wide diversity in the various state laws regarding electronic signatures is hindering the development of e-commerce, new business models, or new technologies, and whether the lack of uniform state or federal e-commerce legislation is putting the U.S. at a competitive disadvantage.

147. Examples include credit card-based sales of consumer products (i.e. amazon.com) and as online stock trading.

History has shown us that Mexico's delay in reforming its divergent mix of secured transactions laws to provide predictability and keep pace with the legal innovations of countries such as the U.S. and Canada greatly inhibited the extension of credit in Mexico and thereby hindered its economic growth. We would do well not to make the same mistake with our electronic signature laws.

One thing is certain: great change predominates the e-commerce world, and unless we move with change, we will become its victims.