Chicago-Kent Law Review

Volume 76
Issue 3 *Symposium on the Structures of Care Work*

Article 21

April 2001

The E-Sign Act: The Means to Effectively Facilitate the Growth and Development of E-Commerce

Scott R. Zemnick

THE E-SIGN ACT: THE MEANS TO EFFECTIVELY FACILITATE THE GROWTH AND DEVELOPMENT OF E-COMMERCE

SCOTT R. ZEMNICK*

INTRODUCTION

We are currently living through a revolution of electronic communication and digital information technology equal in magnitude to the revolution of television in the 1950s and 1960s. In this new world of electronic communication and digital information, new Internet technologies, such as e-mail, the World Wide Web, and Electronic Data Interchange ("EDI"), are rapidly becoming integral parts of commercial life. Consequently, electronic commerce ("e-commerce")[1] is quickly enhancing or replacing other forms of traditional commercial activity in both business-to-business and business-to-consumer interactions.

The sheer impact of e-commerce is forcing businesses to redefine their corporate strategies and to redesign their business models. Businesses are using the Internet in increasing numbers because of the unique commercial opportunities e-commerce offers over the traditional means of commercial activity.[2] In fact, the value of U.S.-based e-commerce transactions was estimated to be $43 billion in 1998 and is projected to increase to $3.2 trillion by 2004.[3] Such an

* J.D., Chicago-Kent College of Law, Illinois Institute of Technology, 2001; B.A., University of Michigan, 1998. The author wishes to thank L. Daniel Liutikas for his editorial assistance.

1. "'Electronic commerce' can be generally defined as the business environment in which the advertising, buying, and selling and/or licensing of goods, services and/or information occurs electronically, such as through the use of computer networks or wireless communication systems." Holly K. Towle, *Electronic Transactions and Contracting, in* SECOND ANNUAL INTERNET LAW INSTITUTE 515, 517 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. 520, 1998).

2. The Internet enables businesses to "reduce distribution and marketing costs . . . [to] eliminate the middleman . . . [to] increase efficiency, promote impulse transactions and streamline distribution to far-flung locales . . . [to] connect directly with consumers at home . . . [to] streamline operations and internal transactions, and [to] increase business-to-business sales." Margaret Littman, *Cyberspace Race: Online Sales Projected to Reach $368 Billion in 2002*, CRAIN'S CHI. BUS., Nov. 30, 1998, at SR1.

3. *See* CyberAtlas, *Latin American E-Commerce Showing Signs of Growth, at*

increase, however, is not only limited to U.S.-based e-commerce transactions. E-commerce transactions are also projected to drastically increase worldwide. According to projections by one research firm, worldwide e-commerce sales will grow from $145 billion in 1999 to as high as $7.8 trillion in 2004.[4]

E-commerce is not only forcing companies to redefine the means of conducting their business, but it is also changing the basic legal infrastructure. There is currently an enormous amount of activity underway by the states to clarify the law regarding the conduct of e-commerce transactions.[5] The enforceability of e-commerce transactions is the most basic and fundamental issue that current state legislation addresses, generally in the form of electronic signature legislation.[6] Though the various legislative initiatives show an agreement among the states to further facilitate e-commerce, there is little agreement among the states on how to attain such a goal.[7] Consequently, the following question challenges lawmakers today: What type of legislation, if any, will be effective in facilitating the growth and development of e-commerce?

Part I of this Note discusses the anatomy of electronic transactions. It includes an overview of the three methods of information transfer most commonly involved in electronic transactions over the Internet: (1) ASCII text files, which are used primarily in e-mail communications; (2) binary files, which are used primarily on the World Wide Web; and (3) EDI.

Part II begins with a discussion of the differences between electronic communication and traditional paper-based communication, specifically their differences in (1) malleability; (2) transmissibility; and (3) processibility. It then discusses the various legal issues that arise from these differences, including (1) authenticity; (2) integrity; (3) nonrepudiation; and (4) the writing and signature requirements.

http://cyberatlas.internet.com/big_picture/geographics/print/0,1323,5911_348161,00.html (last visited Mar. 1, 2000).

4. *Id.* By 2004, business-to-business e-commerce will represent 8.6% of worldwide sales of goods. *Id.*

5. For a list of legal initiatives, see the Web site of McBride, Baker & Coles, a Chicago law firm, at www.mbc.com, which provides a regularly updated summary of all enacted and pending electronic and digital signature legislation. As of August 29, 2000, Massachusetts and Michigan are the only states that have not introduced any electronic or digital signature legislation. *See id.*

6. In the U.S. alone, fifty-seven new electronic signature bills were introduced in the state legislatures during the first two months of 1999. *See id.*

7. *See id.*

Part III discusses the various state legislative initiatives that currently exist with respect to electronic signatures. It discusses the two broad categories of state legislation relating to electronic signature technology. It then discusses the types of transactions covered by the current signature legislation. It then examines the Uniform Electronic Transactions Act ("UETA"), which numerous states have recently enacted.

Part IV discusses the Electronic Signatures in Global and National Commerce Act ("E-Sign Act") and examines its most significant provisions.

Finally, Part V argues that the current state electronic signature legislation, including the UETA, is hindering, rather than facilitating, the growth and development of e-commerce. Part V argues that the E-Sign Act will solve the problems caused by the conflicting state legislation, by providing the uniformity, flexibility, and predictability necessary to facilitate the growth and development of e-commerce.

I. THE ANATOMY OF ELECTRONIC TRANSACTIONS

Electronic communications encompass three methods of information transfer: (1) free text file, commonly known as ASCII code, which is primarily transmitted in direct e-mail communications; (2) binary files, which are primarily transmitted over the World Wide Web in what is known as File Transfer Protocol ("FTP"); and (3) EDI.

A. ASCII Text File and E-Mail

The most familiar and the simplest form of electronic communication is an ASCII text file.[8] ASCII (American Standard for Character Information Interchange) enables users to compose any message they want by assigning a particular machine-readable number to each letter in the alphabet, common punctuation marks, and each Arabic numeral.[9] Because of the simplicity of ASCII text files, they are easier and faster to transfer than binary files.[10] The simplicity of ASCII text files, however, also has its limitations. ASCII text files can only transfer text in very sparse form, which prevents the

8. *See* YOCHAI BENKLER, LEGAL RESEARCH NETWORK, INC., RULES OF THE ROAD FOR THE INFORMATION SUPERHIGHWAY: ELECTRONIC COMMUNICATIONS AND THE LAW 10 (1996).

9. *See id.*

10. *See id.*

transmission of more complex text and "simple" word-processing codes.[11]

In addition, the simplicity of ASCII text files enables them to be used for direct e-mail communications, which makes ASCII text files the method of communication most commonly known to users.[12] Businesses and other users of the Internet are increasingly seeking to use e-mail to conduct commercial activity at a distance because of the numerous advantages e-mail has over the postal service, private carriers, telephones, and facsimiles. E-mail offers businesses the opportunity to communicate and exchange any information that can be stored electronically without the constraints of physical locations.[13] E-mail is also quicker and cheaper than the alternative means of communication.[14] Consequently, e-mail is fast becoming the preferred method for business interaction.

B. Binary Files, FTP, and the World Wide Web

Binary files include information, such as computer programs, music, color, sound, and complex formatting instructions and language presentations, which cannot be transferred in ASCII text files because of their complexity.[15] All digital information can be reduced to binary files.[16] Binary files are most commonly transferred in FTP, because FTP enables the user to send and receive complex files that are not or cannot be presented in ASCII text files.[17]

With the recent rapid growth of the World Wide Web,[18] binary files have become extremely popular among users. As one author noted, "[t]he transfer of binary files permits an infinite variety of information to be distributed to any user."[19] Internet users can search and link files in binary form. Therefore, Internet users can transfer both simple and complex binary forms, such as text, music, and video

11. *See id.* Underlining, italicizing, columns, and graphics are examples of "simple" word processing codes.

12. *See id.*

13. *See* JULIAN S. MILLSTEIN ET AL., DOING BUSINESS ON THE INTERNET: FORMS AND ANALYSIS 8-4.2 (1997).

14. *See id.*

15. BENKLER, *supra* note 8, at 11.

16. *See id.*

17. *See id.*

18. The percentage of the U.S. population who uses the World Wide Web increased from 41% in January 1999 to 56% in December 1999, an increase of 15% in one year. Harris Interactive, *No Slacking in U.S. Net Growth*, *at* http://www.e-land.com/estats/020800_harris.html (last visited Mar. 1, 2000).

19. BENKLER, *supra* note 8, at 12.

graphics, to other Internet users.[20] For example, multiple Internet users can receive binary files with on-screen text and high quality pictures from remote databanks.[21] Consequently, the rapid development of the World Wide Web and the popularity of binary files may "come to fulfill a role very similar to that of cable, broadcast, and newspapers in the mass media culture."[22]

C. *Electronic Data Interchange*

Though e-mail and the World Wide Web present new mediums for commercial activity, businesses have been using computers and telecommunications networks for years. Traditionally, businesses with well-established relationships use EDI to link their computer systems and electronically transmit business documents, such as purchase orders, invoices, and receipts.[23] EDI is the transfer of data between different companies using networks, such as the Internet.[24] The messages and data transmitted by the computer systems are highly structured and follow prearranged formats capable of being automatically processed by the computer systems.[25] Consequently, the computer systems can conduct commercial transactions without human intervention.[26] Therefore, EDI permits businesses to increase the speed and efficiency of transactions.

20. *See id.* at 11.

21. *See id.* at 12.

22. *Id.*

23. *See* MILLSTEIN ET AL., *supra* note 13, at 8-5. A typical EDI transaction is conducted as follows:

> [A] buyer would format and transmit an electronic purchase order setting forth information, which would normally be included in a paper-based order, such as the company name, address, a description of the goods being ordered and a means for delivery. The buyer would then electronically send the purchase order to the supplier. Upon receipt, the supplier would transmit an electronic confirmation to the buyer to verify that the communication received is accurate as to its terms. Upon receiving a return communication from the buyer confirming the order, the supplier would then send another transmission to the buyer to indicate its acceptance (or rejection) of the order.

Id. at 8-6.

24. *See* Webopedia: Online Computer Dictionary for Internet Terms and Technical Support, *at* http://webopedia.internet.com/TERM/E/EDI.html (last visited Mar. 1, 2000).

25. *See* BENKLER, *supra* note 8, at 12.

26. The following is an example of how computer systems involved in EDI can conduct commercial transactions without human intervention:

> [A] manufacturer can set up its computer system so that, when its supplies drop below a certain threshold, its computer system automatically formats and sends a purchase order to the proper supplier. The supplier's computer system, upon receipt of the message, can be set up to automatically process the order and arrange for its fulfillment.

MILLSTEIN ET AL., *supra* note 13, at 8-6.

Though speed and efficiency are advantageous, the primary benefits of EDI are its clarity and recordability.[27] First, EDI communications are much less likely than paper-based transactions to be ambiguous because EDI communications cover a specific set of transactions, which have been explicitly listed and previously agreed upon in a contract by the parties.[28] In addition, EDI communications enable parties to immediately confirm the receipt and accuracy of an order.[29] Consequently, disputes about the content of a particular transaction are rare because EDI communications can provide reliable records of past transactions.[30]

II. THE LEGAL ISSUES ARISING FROM ELECTRONIC TRANSACTIONS

The move from paper-based to electronic communication technologies has given businesses many commercial advantages. However, this shift in technology also raises many legal issues, including authenticity, integrity, nonrepudiation, the writing requirement, and the signature requirement.

A. Electronic Communication and Digital Information Differ from Traditional Paper-Based Methods of Communication

Electronic and digital communications represent a text, image, or sound, originally stored in a form readable only by machines, in a manner comprehensible to humans.[31] Three inherent advantages of electronic communications and digital information differentiate them from the traditional paper-based methods of communication and human interaction: (1) malleability, (2) transmissibility, and (3) processibility.

1. Malleability

Electronic communications and digital information are extremely malleable. Alterations to the text of paper-based communications can be obvious to the naked eye. However, unlike the text of paper-based communications, the text of an authentic electronic

27. *See* BENKLER, *supra* note 8, at 13.
28. *See id.*
29. *See* MILLSTEIN ET AL., *supra* note 13, at 8-6.
30. *See* BENKLER, *supra* note 8, at 13.
31. *See id.* at 31.

communication contains no inherently distinctive characteristics that would distinguish it from the text of a copy, forgery, or an altered version of that electronic communication.[32] Thus, alterations and forgeries of electronic communications are extremely difficult to detect with the naked eye.

In addition, unlike paper-based communications, in which the message and the medium are transmitted together in a tangible, physical object, electronic communications are disembodied from a tangible medium.[33] Consequently, while the electronic information is being stored on a computer, unauthorized people can gain access to a computer system and then retrieve, alter, and save information as an original file without any signs of tampering. This unauthorized tampering can occur before the recording of the original message to a tangible medium.[34]

2. Transmissibility

Electronic signals are also extremely transmissible. First, electronic communications and digital information are transmitted through either wires or microwaves.[35] However, because transmission involves many transfer points, such as packet-switching nodes,[36] anyone that can access these various transfer points can intercept, alter, and retransmit the altered version.[37]

In addition, computer hackers and anonymous senders often make it extremely difficult to determine who sent an electronic message. Computer hackers can break into a computer network and easily trick the network into sending a communication with the address of another individual that did not actually send the

32. *See* Thomas J. Smedinghoff, *Digital Signatures: The Key to Secure Internet Commerce*, *in* ONLINE AND INTERNET LAW 201, 211 (1998).

33. *See id.*

34. *See id.* at 211-12. In contrast, paper-based communications use a variety of features that make alterations to the original easy to detect, such as the use of chemically treated or patterned paper, special inks, and unique printing styles or processes. *See id.* at 211.

35. *See* BENKLER, *supra* note 8, at 32.

36. *See* Smedinghoff, *supra* note 32, at 211. Packet-switching nodes are processing locations within a network where messages are divided into parts, called packets, before they are sent. *See* Webopedia: Online Computer Dictionary for Internet Terms and Technical Support, *at* http://webopedia.internet.com/TERM/P/packet_switching.html (last visited Mar. 1, 2000). Each packet is then transmitted individually and can follow different routes to its destination. *See id.*

37. *See* Smedinghoff, *supra* note 32, at 211-12.

communication.[38] An individual can also send a message anonymously,[39] which makes it impossible for the recipient to know the sender.

Furthermore, electronic communications are often conducted over open networks,[40] which lack adequate access and usage controls.[41] Consequently, various people can use these networks to access other systems connected to the network to intercept and possibly alter electronic transactions.[42] Finally, unpredictable transmission errors can also change the original electronic communication.[43]

3. Processibility

The processibility of electronic communications enables individuals to store and retrieve increased amounts and types of information that were impossible to process before the advent of computer technology.[44] Electronic communication offers the capacity to communicate over distances and speeds once thought impossible. Because of this emerging technology, an increasing number of people are using computers to store and express their thoughts and ideas in digital and electronic form, rather than using traditional paper-based means. Consequently, an overwhelming amount of people's thoughts and ideas are now subject to search, retrieval, and examination by others with whom they never intended to communicate.[45]

B. The Legal Issues Caused by the Inherent Characteristics of Electronic Transactions

Because of the inherent differences between paper-based and electronic communications, the following legal issues arise when

38. L. Daniel Liutikas, Presentation on the Legal Aspects of E-Commerce before the E-Commerce Task Force at Much Shelist Freed Denenberg Ament & Rubenstein, P.C. (Jan. 12, 2000).

39. Some networks allow a user to send email without identifying himself or herself by email address or username. *See* Webopedia: Online Computer Dictionary for Internet Terms and Technical Support, *at* http://webopedia.internet.com/TERM/A/anonymous_ftp.html (last visited Mar. 1, 2000).

40. Open networks are networks that do not require a user to enter a username or password, or merely permit one to enter the word "guest" to gain access. *See id.*

41. *See* Smedinghoff, *supra* note 32, at 214.

42. *See id.*

43. *See id.*

44. *See* BENKLER, *supra* note 8, at 33.

45. *See id.* at 34.

transacting electronically: (1) authenticity, (2) integrity, (3) nonrepudiation, and (4) the writing and signature requirements.

1. Authenticity

Authentication is the process of verifying that the people or things that you cannot see are who or what they claim to be.[46] It is the most essential element of electronic transactions because it is the basis of access control, of permissions and authorizations, of enforcing accountability, and of achieving nonrepudiation.[47] In the context of electronic transactions, authenticity concerns whether the transaction is from the expected party or whether the transaction is from an imposter trying to transmit a forgery.[48] On the Internet, electronic transactions often occur between parties without preexisting relationships. Therefore, it is often extremely difficult for one party to clearly ascertain the identity of another party with whom it is contracting.[49] Consequently, certain situations involving a party's capacity or authority to form a contract can render a seemingly valid contract unenforceable. Such situations include when a party is a minor or when a party claims to enter a contract on behalf of an employer or organization but lacks the authority to do so.[50]

2. Integrity

Integrity pertains to the accuracy of a communication.[51] In other words, integrity is concerned with whether the communication received is exactly the same as the communication sent.[52] As Thomas J. Smedinghoff, a pioneer of e-commerce legislation, noted: "Integrity is critical to electronic commerce when it comes to the negotiation and formation of contracts online, the licensing of digital content, . . . the making of electronic payments, [and] to proving up these transactions using electronic records of them at a later date."[53]

46. *See* FED. R. EVID. 901(a).

47. Liutikas, *supra* note 38.

48. For example, a merchant does not want its customer's payment deposited to an account of someone impersonating the merchant; and a bank wants to be able to bind a credit card number to its rightful owner. *See* Margaret J. Radin & Daniel L. Appelman, *Doing Business in the Digital Era: Some Basic Issues*, *in* ECOMMERCE: STRATEGY RESOURCES IN THE DIGITAL ECONOMY 51, 55 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. 570, 1999).

49. *See* MILLSTEIN ET AL., *supra* note 13, at 8-7.

50. *See id.*

51. *See* Smedinghoff, *supra* note 32, at 206.

52. *Id.*

53. *Id.* Smedinghoff offers the following example, which demonstrates the importance of

However, the ease with which individuals can access and alter the content of electronic communications transmitted over open networks can have negative consequences. Uncertainty about the accuracy of the content of an electronic transaction can affect contract formation, interpretation, and enforcement.[54] For instance, if contracting parties cannot verify that the electronic communication sent is the same as the communication received, then parties will be able to repudiate otherwise enforceable contracts, hindering the increased efficiency of electronic transactions.[55]

3. Nonrepudiation

Nonrepudiation is a legal requirement where one contractual party seeks to hold another party to the contract.[56] Nonrepudiation is essential to e-commerce in situations where a party is willing to rely on a communication, electronic contract, or a funds transfer request.[57] As explained earlier in this Note, electronic communications are extremely malleable and accessible to outsiders, who can then retrieve and alter the original message. An individual can also hack into a computer network and send a communication with the address of another party. Consequently, parties to electronic transactions may have legitimate claims that one of the parties did not send the communication or that the contents of the communication as received were not the same as originally sent.

Conversely, the malleability and accessibility of electronic communications also give a party the opportunity to repudiate by falsely denying that a transaction occurred or was authorized. If the

integrity in electronic commerce:

> [C]onsider the case of a building contractor who wants to be able to solicit bids from subcontractors and submit its proposal to the government online. The building contractor needs to be able to verify the accuracy of the bids upon which it will rely in formulating its proposal. The building contractor is faced with the problem of how to confirm that the bids as received are accurate.

Id.

In addition, a customer does not want to order a bathmat and receive a bathtub; a bank does not want to sign a digital coin for $0.10 and have it become a $1,000,000 bill. *See* Radin & Appelman, *supra* note 48, at 55.

54. *See* MILLSTEIN ET AL., *supra* note 13, at 8-8.

55. *See id.*

56. *See* Smedinghoff, *supra* note 32, at 206. Repudiation of a contract occurs with words or actions indicating that a party is not going to perform his or her duty or obligation owed to the other party in the future. BLACK'S LAW DICTIONARY 903 (6th ed. 1991).

57. *See* Smedinghoff, *supra* note 32, at 206. For example, a merchant does not want its customer to stop payment after delivery of goods by denying a transaction ever occurred. *See* Radin & Appelman, *supra* note 48, at 55.

sender did, in fact, send a communication, or if the content of communication as received was, in fact, the same as the communication sent, then the sender must not be able to escape his or her legal contractual obligations by repudiating the contract. A somewhat common occurrence of such a situation occurs in "click-wrap" contracts where a user claims that he or she did not click the button to accept the contract or that he or she clicked the button accidentally without intending to do so.[58]

4. The Writing and Signature Requirements

In many cases, the law requires that an enforceable agreement be in "writing" and "signed" by the party the agreement seeks to bind.[59] The Statute of Frauds is an obvious example of such a law.[60] The Statute of Frauds was developed as a means of preventing fraud and perjury by providing proof that the alleged agreement was, in fact, made.[61] In addition, numerous other federal, state, and local statutes and regulations also require that a transaction be in writing and contain a signature.[62]

Satisfying the writing and signature requirements is not a problem for traditional paper-based transactions. However, satisfying the traditional meanings of "writing" and "signature" poses a problem for electronic transactions because these transactions do not involve the traditional use of pen and paper.[63] Consequently, the

58. Click-wrap agreements are common on Web sites. Web sites sometimes require that users electronically accept the terms of an online agreement by means of "clicking" on a box that states "I agree," before the site allows the user to access or download the materials on the site. *See* MILLSTEIN ET AL., *supra* note 13, at 8-38.4.

59. Thomas J. Smedinghoff & Ruth H. Bro, *Moving with Change: Electronic Signature Legislation As a Vehicle for Advancing E-Commerce*, 17 J. MARSHALL J. COMPUTER & INFO. L. 723, 733 (1999).

60. The original Statute of Frauds was an English statute requiring certain kinds of contracts to be in writing. *See* E. ALLAN FARNSWORTH, CONTRACTS 364 (3d ed. 1999). Its primary purpose was to avoid fraudulent claims by requiring a party to produce a writing that would prove the existence of the party's claim. *Id.* Almost all states have enacted their own version of the original Statute of Frauds. *See id.*

Unless additional requirements are imposed by a particular state statute, a contract will satisfy the Statute of Frauds if there is a writing, signed by, or on behalf of, the party to be charged, which: (1) reasonably identifies the subject matter of the contract; (2) is sufficient to indicate that a contract has been made between the parties or that the signing party has made an offer; and (3) states with reasonable certainty the essential terms of the contract. RESTATEMENT (SECOND) OF CONTRACTS § 110 (1981).

61. *See* FARNSWORTH, *supra* note 60, at 366.

62. *See* Smedinghoff, *supra* note 32, at 208. For example, before the government will consider itself bound to a contract, the contract must be in writing and signed. *See* Pub. L. No. 97-258, 96 Stat. 927 (1982).

63. Smedinghoff, *supra* note 32, at 219.

following question confronts electronic transactions: Will electronic transactions, which fall under the Statute of Frauds or other laws requiring an agreement to be in writing and signed, satisfy the writing and signature requirements?

III. CURRENT ELECTRONIC SIGNATURE LEGISLATION

Currently, forty-eight states and the federal government have enacted or are currently addressing the authenticity, integrity, nonrepudiation, and the writing and signature requirement issues raised by electronic signatures.[64] States, which have been legislating in the area of electronic signatures, have expressed the following policies for their activity: (1) to promote and encourage electronic commerce by ensuring the security and reliability of electronic communications; (2) to minimize fraud and forged communications in electronic communications; and (3) to increase public confidence in the use of electronic signatures.[65] Though these policies are common among the various states, each state's legislation greatly differs in its means of achieving these common policies. In analyzing the current body of legislation, it is necessary to distinguish the various statutes by their approaches to electronic signature technology and by the types of transactions they cover.

A. Two Legislative Approaches to Electronic Signature Technology

State legislation relating to electronic signature technology can be divided into two broad categories: electronic signature legislation and secure signature legislation.

1. Electronic Signature Legislation

Electronic signature legislation takes a technology-neutral approach. Electronic signature legislation provides that any symbol or method, regardless of the particular technology used, can create a valid signature if executed and adopted by a party with a present intent to be bound.[66] The states adopting this approach have applied

64. *See* Smedinghoff & Bro, *supra* note 59, at 726. Massachusetts and West Virginia are the only states that have not enacted any signature legislation. McBride, Baker & Coles, E-Commerce Spotlight: State Initiatives, *at* http://www.mbc.com/ecommerce/legislative_1.asp?state=all (last visited Mar. 1, 2000).

65. *See, e.g.*, FLA. DEP'T OF STATE, ELECTRONIC COMPANY IN FLORIDA: REPORT TO THE JOINT LEGISLATIVE COMMITTEE ON INFORMATION TECHNOLOGY RESOURCES (1996).

66. *See* Thomas J. Smedinghoff, *Electronic Contracts & Digital Signatures: An Overview of*

the current Uniform Commercial Code ("UCC") definition of signature: any symbol made with an intent to authenticate.[67] These states simply require that the signature be some sort of electronic symbol or security procedure that displays the intent to authenticate, whether a digital signature[68] or some other form of electronic signature.[69]

2. Secure Signature Legislation

Unlike electronic signature legislation, secure signature legislation confers legal validity on a subset of possible electronic signatures regarded as sufficiently secure to warrant favorable legal treatment.[70] Secure signature legislation focuses on the technology used to create the electronic signature.[71] There are two primary types of secure signature legislation: digital signature legislation and legislation that does not specify a particular technology, but rather prescribes specific authentication attributes.

Digital signature legislation requires the use of public-key cryptography to create a digital signature and does not address any other forms of electronic signatures.[72] Utah was the first state to enact this type of legislation.[73] Digital signature statutes based on the

Law and Legislation, *in* THIRD ANNUAL INTERNET LAW INSTITUTE 125, 165 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. 564, 1999).

67. U.C.C. § 1-201(39) (1987).

68. *See* Smedinghoff, *supra* note 32, at 219. A digital signature is not based upon actual hand-signed instruments, but rather is a "sequence of bits that is created by running an electronic message through a one-way hash function and then encrypting the resulting message digest with the sender's private key." *Id.* A digital signature is derived solely from the document to be digitally signed. *Id.* Therefore, a digital signature is unique for each document signed. *Id.* Any change to the document will produce a different signature. *Id.* A digital signature resembles a string of alphanumeric characters, such as the following: frKcML1QiJJ+72W++44uuuYGyuTWOLnuuYDnY578yub898u89huhy7hbtfvxgvGMMNdxiW MNVikoiPjbiFRnmO76y44ju. *Id.*

69. *See, e.g.*, Illinois Electronic Commerce Security Act, 5 I.L.C.S. 175/5-105 (1999) ("Any 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."); Mississippi Digital Signature Act of 1997, MISS. CODE 1972 ANN. § 25-63-1 (1998) ("Any 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."); Oregon Electronic Signature Act, OR. REV. STAT. § 192.835 (1998) ("Any letters, characters or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing.").

70. *See* Smedinghoff, *supra* note 66, at 168-69.

71. *See id.*

72. Minnesota, Missouri, Utah, and Washington have enacted this type of legislation. *See* McBride, Baker & Coles, *supra* note 64.

73. The Utah act defines a digital signature as:

Utah approach also confer regulatory authority on a state agency to license certified authorities that operate within their jurisdiction.[74] Licensed certified authorities that comply with the requirements of the governing statute are then afforded significant limitations on liability.[75] Furthermore, digital signature legislation requires that the digital signature must have a verifiable certificate issued from a certification authority licensed under the regulations to gain evidentiary presumption.[76]

The second type of secure signature legislation does not specify a particular technology. Rather, the second type of secure signature legislation gives legal effect only to those types of electronic signatures that meet certain authentication attributes.[77] Though the attributes differ among the individual statutes, the attributes commonly require the electronic signature to 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 data in such a manner that if the data is changed, the digital signature is invalidated.[78] Statutes of this type generally confer authority to a state agency to promulgate regulations that define what technology and practices will meet those standards.[79] California, for instance, provides a process whereby additional technologies may be added to an approved list if those technologies meet the standards set by statute and regulation.

B. The Limited Scope of Transactions Covered by the Current Legislation

In addition to categorizing state legislation into electronic signature legislation and secure signature legislation, one must also distinguish state legislation based on the limitations of the transactions it covers. These limitations generally can be categorized

> [The] transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether: (a) the transformation was created using the private key that corresponds to the signer's public key; and (b) the message has been altered since the transformation was made.

UTAH CODE ANN. § 46-3-103(10) (1999).

74. *See id.* § 46-3-201 to 204.

75. *See id.* § 46-3-309.

76. *See id.* § 46-3-406.

77. *See* Smedinghoff, *supra* note 66, at 166.

78. *See id.*

79. *See, e.g.*, CAL. GOV. CODE § 16.5(a)(5) (1999); TEX. GOV. CODE ANN. § 2054.060(b) (1999). One notable exception to this trend is the Georgia statute. *See* GA. CODE ANN. § 10-12-3 (1998).

by the type of parties involved and by the type of transactions conducted. Several states authorize the use of electronic signatures only for certain parties. For example, some states authorize the use of electronic signatures only for transactions involving government entities,[80] whereas other states authorize the use of electronic signatures only for transactions involving a specific private entity, such as a financial institution.[81] In addition, several states authorize the use of electronic signatures only for a certain type or category of transactions, such as tax returns, UCC filings, or medical records.[82]

C. *The Uniform Electronic Transactions Act*

In response to the conflicting state electronic signature legislation, the National Conference of Commissioners on Uniform State Laws ("NCCUSL") drafted and approved the UETA in July 1999 for adoption by the states. The UETA is an electronic record and signature validation statute. It is an "overlay" statute that leaves existing law in place while generally permitting any legal requirement for a "writing" or "signature" to be replaced with an electronic equivalent.[83] The UETA is a procedural, as opposed to a substantive, act. That is, basic rules of law, such as statutory contract law, continue to apply to transactions, whether or not an electronic medium is used.[84]

The basic rules of the UETA are provided in section 7 of the act. First, a record[85] or signature may not be denied legal effect or enforceability solely because it is in electronic form.[86] Second, a contract may not be denied legal effect or enforceability solely because an electronic record[87] was used in its formation.[88]

80. *See, e.g.*, Idaho Electronic Signature and Filing Act, 1998 IDAHO SENATE BILL 1486 (limited to filing an issuing of documents by and with state and local authorities); Indiana Electronic Digital Signature Act, IND. CODE 5-24-2-2 (1998) (limited to transactions with the state); WYO. STAT. § 9-1-306 (1998) (limited to filings with the Secretary of State).

81. *See, e.g.*, Illinois Financial Institutions Digital Signature Act, 1997 ILL. HOUSE BILL 597 (limited to communications between financial institutions and their customers).

82. *See, e.g.*, Electronic Tax Return Filing Act, CODE OF ALA. § 40-30-5 (1998) (limited to electronic filing of tax returns or other documents with the Department of Revenue); COLO. REV. STAT. ANN. § 4-9-413 (1999) (limited to electronic filings of UCC financial statements); LA. REV. STAT. ANN. § 40:2144 (1999) (limited to medical records).

83. *See* Uniform Electronic Transactions Act ("UETA") § 7 (Proposed Official Draft 1999), *at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm (last visited Mar. 1, 2000).

84. *See id.* § 3(d).

85. A "record" refers to "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." *Id.* § 2(13).

86. *See id.* § 7.

87. An "electronic record" is a "record created, generated, sent, communicated, received,

Furthermore, if a law requires a record to be in writing, an electronic record satisfies the law.[89] Finally, if a law requires a signature, an electronic signature[90] satisfies the law.[91]

The UETA is also technologically neutral. It does not require the use of a digital signature or any other type of security procedure.[92] Therefore, parties are free to use the most up-to-date digital signature technology or less sophisticated security procedures, such as passwords or pin numbers.

Parties are not required to use electronic transactions, electronic records, or electronic signatures.[93] It applies only to transactions in which each party has agreed to conduct the transactions in electronic form.[94] It also contains an "opt-out" provision under which parties may vary, waive, or disclaim most of the provisions of the UETA by agreement.[95] The "opt-out" provision applies even in cases where the parties agreed that transactions would be conducted in electronic form.

Certain types of transactions are excluded from the scope of the UETA. The act excludes transactions to the extent they are governed by (1) the UCC, except for transactions governed by articles 2 and 2A and sections 1-107 and 1-206; (2) the Uniform Computer Information Transactions Act; (3) laws governing estates and trusts; and (4) other laws, if any, identified by the state.[96]

IV. THE ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT

On October 1, 2000, the Electronic Signatures in Global and National Commerce Act ("E-Sign Act")[97] took effect, with the purpose of facilitating the continued success of electronic commerce.

or stored by electronic means." *Id.* § 2(7).

88. *See id.* § 7.

89. *See id.*

90. UETA defines an "electronic signature" as an "electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." *Id.* § 2(8).

91. *See id.* § 7.

92. *See id.* § 2(8).

93. *See id.* § 5(a).

94. *See id.* § 5(b).

95. *See id.* § 5(d).

96. *See id.* § 3.

97. Electronic Signatures in Global and National Commerce Act ("E-Sign Act"), 15 U.S.C. §§ 7001-06, 7021, 7031 (West 2000).

The E-Sign Act preempts any state law that invalidates signatures, contracts, or records relating to interstate or foreign commerce solely because it is in electronic form rather than being on paper.[98] However, all other substantive requirements of state contract law remain in place.[99] This Part examines the most significant provisions of the E-Sign Act.

A. Scope

The E-Sign Act applies to any transaction in or affecting interstate or foreign commerce.[100] A "transaction" is defined broadly as "an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons."[101] It, however, does not apply to several kinds of contracts, agreements, orders, notices, and records that are generally regulated by other state and federal statutes.[102] For example, it does not apply to a contract or other record governed by the UCC, excluding sections 1-107 and 1-206 and articles 2 and 2A. In addition, the E-Sign Act does not apply to transactions governed by laws regulating the creations or adoption of certain testamentary instruments or matters of family law. Furthermore, the E-Sign Act requires all critical notices to be sent in paper-and-ink form.[103]

B. Core Principle: General Rule of Validity

Section 7001(a) sets out the basic rule established by the E-Sign Act. It equates electronic signatures and records with their paper equivalent. It provides that signatures, contracts, and transaction

98. The E-Sign Act, section 7001(a), provides:

> Notwithstanding any statute, regulation, or other rule of law . . . with respect to any transaction in or affecting interstate or foreign commerce:
>
> (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
>
> (2) contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

99. For example, intent to enter into a contract remains a basic requirement of, and is governed by, state contract law, regardless of whether the communications are electronic or paper. *See* Daniel W. Van Horn, *The E-Sign Act: A Move in the Right Direction and a Boost for E-Commerce*, 37 TENN. B.J. 14 (2001).

100. *See* E-Sign Act § 7001(a).

101. *Id.* § 7006(13).

102. *See id.* § 7003(a)-(b).

103. *See id.* § 7003(b)(2).

records cannot be declared invalid simply because they are in electronic form.[104] Consequently, if the parties to a transaction agree on the terms and conditions on which they will accept and use electronic signatures and electronic records in their dealings with one another, a state cannot refuse to give legal effect to the parties' agreement. In addition, the E-Sign Act gives full legal effect to documents required to be "notarized, acknowledged, verified, or made under oath" if the "electronic signature of the person authorized to perform those acts . . . is attached to or logically associated with" the document.[105]

The act defines "electronic signature" as "an electronic sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[106] The definition does not require the use of any particular authentication, encryption, or identification technology. Therefore, the act permits one to use a variety of electronic processes, such as a typed name on an e-mail message or a computerized image of a handwritten signature, as a substitute for an actual handwritten signature.

C. *Consumer Consent*

The E-Sign Act does not require consumers to use or accept electronic signatures, electronic contracts, or electronic records. Rather, the E-Sign Act is based on an "opt-in" policy of public protection, which allows for required information or records to be sent electronically instead of on paper so long as the consumer gives his or her affirmative consent to the use of electronic records and signatures.[107] A "consumer" is defined as "an individual who obtains, through a transaction, products or services that are used primarily for personal, family, or household purposes."[108] Therefore, the consent requirement applies only to business-to-consumer transactions and not to business-to-business transactions.

104. "[A] signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form . . . . [A] contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation." *Id.* § 7001(a).

105. *Id.* § 7001(g).

106. *Id.* § 7006(5).

107. *See id.* § 7001(c).

108. *Id.* § 7006(1).

Under the "opt-in" provision set forth in section 7001(c)(1), if a company wants to use electronic records to conduct a transaction with a consumer, the consumer must affirmatively consent after the company explicitly informs the consumer of the all of the following:

> (1) that the consumer's affirmative consent to receiving records electronically is required before the electronic transaction can proceed;
>
> (2) that the consumer has the right to have the records provided on paper rather than in electronic form;
>
> (3) that the consumer has the right to withdraw consent to receiving records electronically after giving that consent, and whether any consequences will result from the consumer's withdrawal of consent;
>
> (4) whether the consumer's consent, if given, will apply only to the particular transaction to which the electronic records will relate or if it will apply to other identified categories of records that the company will provide or make available during its relationship with the consumer;
>
> (5) about the process through which the consumer may withdraw his or her consent to receiving records electronically;
>
> (6) about the process through which the consumer may modify or update his or her contact information, which the company needs to be able to communicate with the consumer electronically;
>
> (7) about the process through which the consumer may request and obtain a paper copy of an electronic record, and the company must state whether a fee will be charged for fulfilling such a request; and
>
> (8) about the specific hardware and software that the consumer will need in order to access and retain the electronic records to be sent to the consumer by the company.[109]

The validity and enforceability of an electronic record or contract cannot be denied solely because of the failure to obtain electronic consent or confirmation of consent.[110] However, if the consumer affirmatively consents to receiving records electronically after the company informs the consumer of the above information, then the E-Sign Act guarantees the validity and enforceability of the electronic record.[111]

The consumer's consent must be electronic or be confirmed electronically in a manner that "reasonably demonstrates" that the consumer will be able to receive and access the various forms of

109. *Id.* § 7001(c)(1)(B)-(C).
110. *See id.* § 7001(c)(3).
111. *See id.* § 7001(c).

electronic records to which the consent applies.[112] For example, a consumer can "reasonably demonstrate" an ability to access and retain electronic records by opening and returning a test document or by sending an e-mail confirming that he or she has such ability.[113] Similarly, showing that the consumer actually accessed and retained the electronic records can also satisfy the "reasonable demonstration" requirement.[114] However, the consent of a consumer only applies to the particular transaction that gave rise to the obligation to provide the record.[115] A consumer still retains the right to receive all future documents on paper.[116]

D. Retention of Electronic Contracts and Records

Except in cases involving consumer protection disclosure rules, the E-Sign Act generally places no restrictions on when electronic signatures and records within its scope satisfy writing requirements. An exception to this rule is the act's retention requirement. Under the E-Sign Act, an electronic contract or record is satisfactorily retained if (1) the electronic record or contract accurately reflects the information set forth in the contract or record required to be retained; and (2) the electronic record or contract is created in a form that is capable of being retained and accurately reproduced for later reference by all persons who have a right to retain or reproduce the record.[117] This rule permits a state law to deny enforceability if the record does not meet the retention requirement, but it does not require this result.[118]

E. Electronic Agents

The E-Sign Act does not deny validity to records produced automatically by computer programs in response to a consumer's communications. The E-Sign Act uses the term "electronic agent" to

112. *Id.* § 7001(c)(1)(C)(ii).

113. *See* Stephanie Tsacoumis & Victoria P. Rostow, *E-Sign Your Life Away: Digital Signatures in the New Economy*, 4 WALLSTREETLAWYER.COM: SEC. ELECTRONIC AGE 17 (2000).

114. *Id.*

115. *See* E-Sign Act § 7001(c)(1)(B)(ii).

116. *See id.* § 7001(c)(1)(B)(i).

117. *See id.* § 7001(d)(1).

118. "[T]he legal effect, validity, or enforceability of an electronic record . . . *may* be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record." *Id.* § 7001(e) (emphasis added).

refer to "a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response."[119] The E-Sign Act explicitly grants legal validity and enforceability to electronic records created by electronic agents, so long as the action of the electronic record is legally attributable to the person to be bound by the record.[120]

F. Preemption of State Law

Section 7002 of the E-Sign Act prescribes specific conditions under which a state may preserve its own existing or future statutes, regulations, or other rules of law, dealing with the use and acceptance of electronic signatures and records. A state statute, regulation, or rule of law may modify, limit, or supersede the basic rules in section 7001 of the E-Sign Act if it satisfies either of the following two cases. First, the state action enacts the UETA as approved and offered for enactment by the NCCUSL in 1999, provided any additional exclusions under UETA § 3(b)(4)[121] are consistent with Titles I and II of the E-Sign Act.[122] Second, the state action specifies alternative procedures or requirements for the use or acceptance of electronic signatures or records for establishing legal effect, validity, and enforceability of contracts or records, and those alternative procedures or requirements are (1) consistent with the E-Sign Act; and (2) do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technological specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic signatures or records.[123]

V. THE E-SIGN ACT WILL EFFECTIVELY FACILITATE THE GROWTH AND DEVELOPMENT OF E-COMMERCE

Our legal infrastructure was designed around a paper-based society. Unfortunately, such a system simply cannot keep pace with

119. *Id.* § 7006(3).

120. *See id.* § 7001(h).

121. Section 3(b)(4) of the UETA allows states to exclude from the scope of the UETA such laws as the state deems appropriate.

122. E-Sign Act § 7002(a)(1).

123. *See id.* § 7002(a)(2)(A).

the technological developments associated with electronic communications. Through legislation, states are currently attempting to provide a legal infrastructure that will support the use of security procedures with the public policy goal of further facilitating the growth and development of e-commerce.[124]

However, in this attempt, rather than establishing clear legal standards, the current state legislation creates more confusion. State electronic signature legislation prescribes conflicting technologies and covers different transactions.[125] Rather than facilitating the growth and development of e-commerce, the current state electronic signature legislation prevents businesses and consumers from reaping the benefits of e-commerce, most notably decreased transaction costs, speed, efficiency, and the means to vast economic opportunities.[126]

Unlike the current state electronic signature legislation, the E-Sign Act offers three key components that will help it achieve the public policy goal of the growth and development of e-commerce: (1) uniformity; (2) flexibility; and (3) predictability.[127] These components will eliminate the obstacles to efficient interstate electronic transactions posed by the conflicting states' laws, particularly the various versions of the UETA, which numerous states have adopted.

A. Uniformity among the States Will Destroy the Barriers Imposed by the Current Conflicting State Legislation

Though the NCCUSL drafted the UETA with the goal of uniformity among the states, two problems have prevented the UETA from achieving this goal. First, the states have not moved quickly enough to enact the UETA. Despite approval by the NCCUSL, a uniform law is not law anywhere in the United States. It is simply a legislative proposal addressed to the fifty state legislatures, who then must individually enact the uniform law. Uniformity cannot be achieved unless all fifty states adopt the UETA. At the time of this Note's publication, nearly two years after the NCCUSL completed its work on the UETA, only twenty-five states had

124. *See, e.g.*, FLA. DEP'T OF STATE, *supra* note 65.

125. *See* LA. REV. STAT. ANN. § 40:2144 (limited to medical records); UTAH CODE ANN. § 46-3-103 (limited to digital signatures only); 5 I.L.C.S. 175/5-105 (authorizing the use of any electronic signature).

126. *See* Littman, *supra* note 2.

127. *See* Smedinghoff & Bro, *supra* note 59, at 761.

adopted versions of the UETA. Consequently, until the UETA is adopted by all fifty states, the lack of uniformity poses a barrier to the growth and development of e-commerce.

Second, even if all fifty states adopted the UETA, each state, as with any uniform law, is free to adopt the UETA with changes. Though some states have adopted near-identical versions of the UETA as proposed by the NCCUSL, other states have adopted the UETA with nonuniform provisions. California, for example, which was the first to enact the UETA, passed a significantly nonuniform version of the UETA. California's version of the UETA made an agreement to electronically transact inadequate to trigger the rules of the UETA if the agreement was contained in a standard form written contract whose primary purpose did not concern electronic transactions.[128] Therefore, parties cannot rely on the California statute to validate a term in a standard form written contract that requires transactions to be sent electronically if the state law requires the transaction to be in writing.

Unlike the current state electronic signature legislation, the E-Sign Act will destroy any barriers between the states that are caused by the conflicting legislation, because it instantly provides baseline uniformity among the fifty states. Uniformity among state and federal law will give parties engaged in e-commerce the certainty that electronic signatures and electronic contracts will have the same legal effect, validity, and enforceability as paper signatures and contracts. The E-Sign Act contains a potent preemption provision that explicitly preempts all state e-commerce laws that are inconsistent with its provisions.[129] Consequently, the E-Sign Act encourages e-commerce among the states because every state would have the same law regarding the legality and validity of electronic signatures.

B. Flexibility Will Enable the E-Sign Act to Adapt to Emerging Technologies

Legislation should neither require nor assume a particular technology by which a party can legally sign or certify electronic transactions. The electronic signature industry needs time to develop before the government can extensively regulate it. Because law, in general, cannot anticipate the development of future technologies,

128. *See* California Uniform Electronics Transactions Act, 1999 CAL. SENATE BILL 820 (1999).

129. *See* E-Sign Act § 7002(a).

the law needs to remain flexible to adapt to the emerging technologies that are certain to develop over time. The E-Sign Act contains the flexibility necessary to enable the law to adapt to emerging technologies as it explicitly preempts any state e-commerce law that is biased against any particular form of electronic signature or electronic document technology.[130]

Some commentators, however, express the fear of inadvertently granting technology that does not give a commensurate level of security, legal protection.[131] However, proscriptive, technology-specific legislation will have the unintended consequences of precluding other authentication technologies and, thus, inadvertently favoring a particular technology.

One can perceive these unintended consequences in the following example. Consider a statute that expressly states that signatures using PKI asymmetric cryptography will have presumed legal validity; assume further that this statute does not explicitly address any other signature technologies. Silence regarding technology X in the face of explicit reference to technology Y could imply the exclusion of technology X from the benefit of presumed legal validity. Therefore, one could assume that the statute in this example grants the presumption of legal validity only to PKI asymmetric technology. Parties would not likely want to take the risk of their transactions becoming legally invalid merely because they used a type of signature technology not explicitly prescribed by the statute. Consequently, parties would likely use only PKI asymmetric technology because the statute explicitly guarantees the presumption of legal validity.

Such a consequence would prevent the development of an equivalent or even a superior level of signature technology. Why use new technologies unless one is certain that a statute will expressly grant the presumption of legal validity to those technologies? Business parties would not likely use new technologies if legislation granted a presumption of legal validity to other technologies. Consequently, legislation that restricts legal validity to specific technologies will only prevent the development of new superior technology, and thus, will impede the growth and potentially the development of e-commerce.

130. *See id.* § 7002(a)(2)(A)(ii).

131. *See* Reporter to the Uniform Electronic Transactions Act Drafting Committee, Memorandum (Sept. 18, 1998), *available at* http://www.law.upenn.edu/library/ulc/uecicta/eta1098m.html.

C. *Predictability Will Spark the Growth and Development of E-Commerce*

According to Thomas J. Smedinghoff, "[p]redictability is a watchword for the growth of commerce, and law can play a key role in providing this valuable commodity."[132] With the advent of new electronic signature technologies, parties engaging in electronic transactions will face legal challenges that will test the limits of current statutory and case law.[133] Consequently, the lack of predictability in the law can have numerous negative consequences for businesses trying to reap the benefits of e-commerce.

First, unpredictability leads to increased litigation.[134] Increased litigation would particularly hurt small start-up companies who could least afford litigation costs. In addition to the legal costs involved in litigation, litigation can also damage business relationships, create adverse publicity, and cause a loss of goodwill.[135]

To avoid litigation, businesses will have to attempt to predict every possible issue that could exist in a transaction without having a firm understanding of the law from which these issues would arise. This would drastically increase the time spent preparing the transaction, increasing transaction costs and decreasing business efficiency.[136] Consequently, the lack of predictability in current electronic signature legislation poses too many risks that would deter many businesses from using e-commerce.

Unlike the current legislation, the E-Sign Act will establish the predictability necessary for the growth and development of e-commerce. The E-Sign Act treats electronic transactions and electronic signatures as legally equivalent to paper-based transactions and signatures, no matter the technology used. Therefore, parties will be able to conduct their business by means of electronic transactions without the fear of potential litigation based merely on the type of technology used. Consequently, the E-Sign Act will offer the predictability that businesses require before they engage in and benefit from e-commerce.

132. Smedinghoff & Bro, *supra* note 59, at 753.
133. *See id.* at 754.
134. *See id.* at 760.
135. *See id.*
136. *See id.* at 759.

D. Implementing Simple Procedural Changes Will Easily Overcome the Possible Legal Issues Caused by the E-Sign Act

The principal attacks on nonrestrictive legislation like the E-Sign Act center on security issues, the ease of entering into electronic contracts, and the ease of transmitting electronic transactions. First, under the E-Sign Act, a party could be held liable for the unauthorized transactions made by another party who unlawfully obtained access to its signature device.[137] For instance, if a party somehow failed to protect the security of its signature device, such as its private key, then that party could be held liable for transactions made through the unauthorized use by another party. Although such liability could be severe, contracting parties should have the right and freedom to make and accept a binding agreement in an electronic medium that will be enforced by the sanctions at law, also known as the concept of "liberty of contract."[138]

Second, the ease with which parties can enter into electronic transactions could cause a party to unintentionally enter into a binding agreement. Therefore, critics would likely favor a restrictive piece of electronic signature legislation that places more hurdles in forming a legally valid contract. However, such criticism is flawed because entering into a paper-based contract is as easy as entering into an electronic-based contract. A handwritten signature required by a paper-based contract is no more burdensome than a click on the "yes" icon required by a "click-wrap" contract.

In addition, a party can easily take precautions to prevent unintentional acceptances without the intervention of a restrictive piece of legislation. For instance, to emphasize that a user is entering into a binding contract, a contracting party can merely bold a statement directly above the signature line, stating "ACCEPTANCE OF THIS AGREEMENT IS LEGALLY BINDING, AND YOU WILL BE LIABLE FOR ALL INSTANCES THAT MIGHT FLOW FROM THE ACCEPTANCE OF THIS AGREEMENT." Furthermore, instead of simply requiring a click on the "yes" icon as the means of acceptance, a party can simply require the other party to type the word "yes" in a designated area. It could be argued that requiring a party to type the word "yes" forces the signer to be more diligent in his or her actions.

137. *See id.* at 755.
138. BLACK'S LAW DICTIONARY 633 (6th ed. 1991).

Finally, the ease with which a party can negligently transmit an electronic transaction to a third party could be of some concern. The following example using the attorney-client privilege best displays the detrimental consequences that can arise from the ease of transmitting electronic transactions.

Consider an attorney and his client communicating by e-mail regarding the client's case. Though the attorney-client privilege gives the client the right to require his or her attorney not to disclose confidential information communicated in the attorney-client relationship, the client can waive this privilege.[139] If a client negligently forwards e-mail from his or her attorney, regarding confidential information, to a friend, then the client has waived his or her attorney-client privilege, and the opposing party can require the client to disclose the information contained in the e-mail in court.[140]

However, parties can prevent the negligent forwarding of electronic transactions by implementing a proprietary inbox system. A proprietary inbox system places more hurdles to forwarding an electronic communication than a common e-mail system. Similar to a common e-mail account, only a member of a proprietary inbox system can access his or her e-mail.[141] However, unlike a common e-mail account, in which a user can forward his or her e-mail to an infinite number of people with a simple click of a button, a member of a proprietary inbox system can only forward his or her e-mail to other members of the inbox system.[142]

Proprietary inbox systems place a further hurdle to forwarding e-mail by requiring members to perform multiple steps before being able to forward e-mail. A member of a proprietary inbox system must download the received e-mail and then attach the message contained in that e-mail to a new e-mail before sending it to someone outside the proprietary inbox system.[143] Furthermore, a proprietary inbox system can be programmed to automatically include a bold statement with every electronic message that reads: "WARNING! FORWARDING THIS MESSAGE TO THIRD PARTIES COULD LEAD TO LIABILITY AND OTHER UNINTENDED CONSEQUENCES, SUCH AS THE LOSS OF AN ATTORNEY-CLIENT

139. *See* FED. R. EVID. 501.

140. *See id.*

141. Interview with L. Daniel Liutikas, Chair, E-Commerce Task Force, Much Shelist Freed Denenberg Ament & Rubenstein, P.C. (Mar. 31, 2000).

142. *Id.*

143. *Id.*

PRIVILEGE. TAKE EXTRA CARE IN FORWARDING THIS MESSAGE TO A THIRD PARTY."[144] These additional hurdles will likely cause less negligence among users in forwarding electronic messages and, thus, prevent any unintended consequences of transmitting electronic communications.

CONCLUSION

The future of commerce will not take place on paper. Rather, it will take place through electronic communications and digital technology information. Although the law cannot successfully predict the future of technological developments, the law can grow and adapt with them. The E-Sign Act offers a simple solution to the legal issues raised by the emerging electronic society. By giving the electronic medium the same legal effect, validity, and enforceability as the medium of paper, the E-Sign Act will prove to be the means to successfully facilitate the growth and development of e-commerce.

144. *Id.*