E-Sign: Paperless Transactions in the New Millennium

Steven Domanowski

Follow this and additional works at: https://via.library.depaul.edu/law-review

Recommended Citation
Steven Domanowski, E-Sign: Paperless Transactions in the New Millennium, 51 DePaul L. Rev. 619 (2001)
Available at: https://via.library.depaul.edu/law-review/vol51/iss2/18

This Comments is brought to you for free and open access by the College of Law at Via Sapientiae. It has been accepted for inclusion in DePaul Law Review by an authorized editor of Via Sapientiae. For more information, please contact wsulliv6@depaul.edu, c.mcclure@depaul.edu.
E-SIGN: PAPERLESS TRANSACTIONS IN THE NEW MILLENNIUM

INTRODUCTION

"Just imagine if this had existed 224 years ago, the Founding Fathers wouldn't have had to come all the way to Philadelphia on July 4th for the Declaration of Independence. They could have E-mailed their 'John Hancocks' in."¹

President William Jefferson Clinton proclaimed the above statement on June 30, 2000. On that day, President Clinton signed—electronically signed—the Electronic Signatures in Global and National Commerce Act (E-SIGN).² E-SIGN lays a new foundation for contract law, giving electronic contracts the same legal enforceability as equivalent paper contracts.³ E-SIGN, which was passed by majorities of both parties in the Senate and House of Representatives, will lead business into the new century with the legal certainty necessary to invest in and expand electronic commerce.⁴

The Founding Fathers understood that the right of individuals to enter into commercial contracts was fundamental, not just for economic growth but also for the preservation of liberty itself.⁵ Great advances in technology, however, have called into question the very basic principles upon which the foundations of contract law are laid. The burgeoning use of the Internet and other electronic transmission systems has resulted in the widespread use of electronic transactions as a standard and popular mode for contracting within the commercial business environment.⁶

⁴. See E-SIGN, Statement by President, supra note 1, at 1561.
⁵. Id.
Technology has often been the motivating factor for change in the arena of commercial law. With the advent of new technology, new business methods arise that require a re-evaluation of the legal framework of commerce. Traditional legal frameworks presume that transactions are paper-based with accompanying signatures. However, offers or acceptances transmitted via an electronic media contain no such signatures. Consequently, satisfaction of the Statute of Frauds becomes an issue.

Part II of this Comment will analyze the history and tradition of the Statute of Frauds, including the prerequisites necessary to satisfy the writing and signature requirements. The Statute of Frauds requires that a contract be both a "writing" and "signed" to garner enforceability pursuant to the Uniform Commercial Code (UCC). No lawsuit has been adjudicated that directly examines whether a contract formed via an electronic transmission satisfies the Statute of Frauds.

There is case law, however, that addresses the writing and signature requirements as applied to various paperless transactions, involving technology such as the telegraph, telex, and fax. The history of this case law will be examined in Part II of this Comment. This section will also investigate and analyze the legislative response, on the state and international levels, to the complexities created by electronic transactions. The fear that this lack of clear authority as to whether an electronic contract is enforceable may have potentially undercut the growth and efficiency of electronic commerce. Therefore, several states in the United States and the United Nations began to implement specific legislation designed to combat the anxiety created by the Statute of Frauds with respect to the enforceability of electronic contracts. The troubling nature of this action commenced by the states was illustrated by the lack of uniformity that existed among the various state legislative initiatives. The regulations developed by the

10. Thomas, supra note 8, at 1149.
11. See infra notes 25-184 and accompanying text.
13. Szafran, supra note 6, at 494.
14. See infra notes 51-130 and accompanying text.
15. See infra notes 131-184 and accompanying text.
16. See infra notes 131-184 and accompanying text.
United Nations created a similar challenge. The United Nation's regulations exhibited a lack of harmonization between both state legislation and the Uniform Electronic Transactions Act.\textsuperscript{18}

Part III will examine E-SIGN, analyzing the Act's general rule, scope, and preemption authority.\textsuperscript{19} Because the lack of harmonization between state legislation and the Uniform Electric Transactions Act threatened the viability of the Internet as an efficient instrument of contract law, many scholars argued vehemently for intervention by the federal government on the basis of protecting interstate commerce.\textsuperscript{20} As a result, E-SIGN was born. The Act finally puts to rest the long debate over whether compliance with the Statute of Frauds is a necessary precursor to the legal enforceability of electronic contracts and signatures. Notwithstanding the pertinent criticism that federal legislation in the area of electronic contracts treads on the states' traditional role as "laboratories of experimentation,"\textsuperscript{21} E-SIGN established uniform foundations necessary to develop legal certainty in the era of ever-expanding technological mediums.\textsuperscript{22}

Part IV will examine the harmonizing qualities of E-SIGN.\textsuperscript{23} The reconciliation of various competing models of electronic signature legislation, such as the digital, proto-digital, minimalist, and Illinois Uniform Electronic Transaction Act models, with the harmonizing effect of E-SIGN's preemption power has lead to a uniform body of electronic signature and electronic record legislation. This harmonization has led to speculation regarding whether it is necessary to repeal the Statute of Frauds.

Part V will anatomize the effect of E-SIGN, specifically the necessary development of authentication technology by the private sector and the resulting exposure to liability.\textsuperscript{24} Although E-SIGN harmonizes the different approaches to the legal enforceability of electronic contracts, it is only the beginning. E-SIGN appropriately leaves the development of comprehensive systems and procedures to manage paperless transactions to the private sector. The innovative Internet technology sector is no doubt prepared for this challenge. Notwithstanding the needs of future development, E-SIGN furthers the quest to create flexibility among traditional paper-orientated contract law

\textsuperscript{19} See infra notes 185-262 and accompanying text.
\textsuperscript{20} Robertson, \textit{supra} note 17, at 508.
\textsuperscript{21} Id. at 510.
\textsuperscript{23} See infra notes 263-349 and accompanying text.
\textsuperscript{24} See infra notes 350-372 and accompanying text.
and finally commences the long process of bringing the legal community up to speed with the pace of business transaction technology.

II. BACKGROUND

The Statute of Frauds has been, and continues to be, the foundation for commercial contracts. The requirements set forth therein for a "writing" and a "signature," have provided the business and commercial sectors with a mechanism for the eradication of potential fraud perpetrated by parties to a transaction. The Statute of Frauds, however, has not been without its faults. With the advent of complex technologies, from telegraphs to email and other electronic communication technology, the Statute of Frauds has been forced to metamorphize from a bedrock contract principle to the foundation of new paperless transactions.

The difficulties faced by the business and commercial sectors through the imposition of the Statute of Frauds to less conventional paperless transactions, facilitated an increased attentiveness by state legislatures and the promulgators of uniform laws to solve the problems associated with the application of traditional contractual thinking to new and burgeoning technologies. The legislation introduced, and later enacted, by the state legislatures, and the Uniform Electronic Transactions Act, helped to calm the anxiety over the integrity and enforceability of electronic contracts. This calm, however, did not last for long. The states, as our system of federalism precipitates, developed legislation which suited the needs of a particular jurisdiction, yet created increased complexities with respect to electronic contracts negotiated and executed on an interstate basis. This confusion led the federal government to pursue a uniform body of law that directly addressed the enforceability and validity of electronic contracts and signatures, E-SIGN.

A. U.C.C. § 2-201: The Statute of Frauds

"The Statute of Frauds is a regulatory device in contract law that requires 'writings' and 'signings' to indicate a party's intentions. It is arguably the most controversial rule in the law of contracts." The Statute of Frauds has a notable pedigree:

In 1677, courts in England prohibited a party to a lawsuit from testifying on his or her own behalf because the possibility of fraud and

perjury. As a result, a party with an otherwise valid defense or claim was provided no recourse by the justice system because the party lacked sufficient means to substantiate the claim or defense. For this reason, the English Parliament enacted ‘An Act for the Prevention of Frauds and Perjuries,’ known today as the Statute of Frauds, which required that certain contracts be in writing to be enforceable. Over 320 years later, the Statute of Frauds continues to exist . . . in nearly all fifty states.

Fulfilling the prophecy of its creation, the Statute of Frauds has proved to be an effective tool in “preventing fraudulent claims from being enforced and protecting against questionable or non-existent oral agreements.” Although originally intended to protect against fraudulent claims, the Statute of Frauds has come into disfavor because it is susceptible to misuse by the parties invoking its technical requirement of a signed writing in order to avoid an otherwise valid oral contract.

The skepticism regarding the Statute of Frauds has evolved to encompass its applicability to electronically created and executed contracts, “given that one of the most significant assumptions integrated into the Code is that commerce generally occurs on paper . . .” The threshold question as to the legal validity and enforceability of electronically-formed contracts is whether the electronic transmission fulfills the “writing” and “signature” requirements of the Statute of Frauds. This is the crucial determination:

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.

The Statute of Frauds is enunciated in section 2-201 of the Uniform Commercial Code (U.C.C.). The provision states:

---

27. Id. at 433.
28. Szafran, supra note 6, at 501.
30. Id. at 146.
31. Id.
A simple reading of the Statute of Frauds does not appear to supply a sufficient analysis of the "writing" or "signature" requirements. However, section 1-201 contains additional definitions. For example, U.C.C. section 1-201 defines "written" or "writing" as including "printing, typewriting or any other intentional reduction to tangible form." The section also defines "signed" as including "any symbol executed or adopted by a party with the present intention to authenticate a writing." Although one may argue that the U.C.C. supplies the information necessary to determine whether an electronically-formed contract satisfies the Statute of Frauds, a general concern over the legality of electronic contracts has persisted.

34. Id. at U.C.C. § 2-601. The entire statute reads:
(1) Except as otherwise provided in this section a contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker.

35. Id. at 1-201(46).

36. Id. at 1-201 (39).

37. Smedinghoff & Bro, supra note 32, at 737.
1. Writing Requirement

Section 2-201 of the U.C.C. requires a writing sufficient to indicate that a contract for sale has been made between the parties.\(^{38}\) Section 1-201(46) states that a writing includes any "printing, typewriting, or intentional reduction to tangible form."\(^{39}\) Comment one of section 2-201 states that "[a]ll that is required is that the writing afford a basis for believing that the offered oral evidence rests on a real transaction."\(^{40}\) The flexible definition afforded "writing" pursuant to the U.C.C. indicates a clear presumption that electronically-formed contracts should constitute a writing.\(^{41}\) An electronic contract can be reduced to tangible form, whether stored on an internal drive or floppy disk.\(^{42}\) "Although one cannot read the data directly in the stored format, it may be viewed upon demand in a readable format, either via video display or by paper reproduction."\(^{43}\) "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."\(^{44}\)

2. Signature Requirement

"A signature is used to accomplish two major tasks: 1) authentication and 2) non-repudiation. In order for a person to be bound by a transaction, she must be the person entering the transaction (authentication) and be willing to be bound by the transaction (non-repudiation)."\(^{45}\) In determining whether an electronic or paper contract was signed by the party against whom enforcement is sought, as required by the Statute of Frauds, the writing must show the requisite intent:

\(^{38}\) U.C.C. § 2-201(1) (1977).
\(^{39}\) U.C.C. § 1-201(46) (1977).
\(^{40}\) U.C.C. § 2-201, cmt. 1. Comment 1 states:
  The required writing need not contain all the material terms of the contract and such material terms as are stated need not be precisely stated. All that is required is that the writing afford a basis for believing that the offered oral evidence rests on a real transaction. It may be written in lead pencil on a scratch pad. It need not indicate which party is the buyer and which is the seller. The only term which must appear is the quantity term which need not be accurately stated but recovery is limited to the amount stated. The price, time and place of payment or delivery, the general quality of the goods, or any particular warranties may all be omitted.
\(^{41}\) Dipaolo, supra note 29, at 147.
\(^{42}\) Id.
\(^{43}\) Id.
\(^{44}\) Id.
The party must have possessed the "present intention to authenticate a writing." 46

Comment thirty-nine to section 1-201 of the U.C.C. states:

The inclusion of authentication in the definition of 'signed' is to make clear that as the term is used in this Act a complete signature is not necessary. Authentication may be printed, stamped or written; it may be by initials or by thumbprint . . . . The question always is whether the symbol was executed or adopted by the party with present intention to authenticate the writing. 47

The established rule is that a signature is whatever symbol, mark, or device one chooses to use as a representative of oneself. 48 There is no requirement that the signature be in any particular form. The type of instrument a party uses to make his signature is also immaterial. 49 Despite the broadly defined element of "signed," the procedure of electronic authentication is debatably a "signature." 50

3. Paperless Transactions and the Statute of Frauds

The legal enforceability of electronically formed contracts cannot be analyzed using traditional case law to determine whether or not an electronic contract fulfills the "writing" and "signature" requirements of the Statute of Frauds. 51 Only case law that involves the determination of whether a paperless transaction meets the requisite requirements of the Statute of Frauds is logically appropriate. "Case law concerning the paperless transmission of documents through telex, telegraph, and facsimile supports the legitimacy of electronic messaging in contract formation." 52 Courts have consistently concluded that messages transmitted by telex and telegram fulfill the signed writing requirement of the Statute of Frauds. 53

a. Telegraph

The year 1844 ushered in a communication revolution. 54 Samuel F. B. Morse transmitted the telegraphic message, "What hath God

---

46. U.C.C. § 2-201.
47. U.C.C. § 1-201 cmt. 39.
48. U.C.C. § 1-201 (39).
50. Dipaolo, supra note 29, at 154.
51. U.C.C. § 2-201.
52. See Wilkerson, supra note 49, at 409.
53. Id. at 410.
It was not long thereafter that American courts were faced with the question of the legal enforceability and validity of telegraphic messages. There is a line of cases that found contracts that were created by telegram enforceable.

In 1896, the New Hampshire Supreme Court in *Howley v. Whipple* "established . . . that an offer and acceptance communicated by telegraph amount to a written contract that satisfies the Statute of Frauds." The court concluded:

> 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 the 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.

*Howley* clearly enunciated the legal validity and enforceability of paperless contracts in the context of the telegram. The central issue in *Howley* involved whether a telegraphic message transmitted between parties involved in a land dispute constituted a contract for the purpose of reaching an agreement with respect to the recognition of the property line. The court clearly recognized the telegraphic message at issue as a "writing."

In its analysis, the New Hampshire Supreme Court applied the evidentiary standards applicable to other writings to telegraphic messages. The message delivered by the sender to the operator, which would normally be considered the original message, was not in fact the "original" message according to the court. The court ex-

---

55. *Id.* at 798.
56. *Id.* In *Durkee v. Vermont Central Railroad Company*, 29 Vt. 48 (1856), an agent brought an action to recover a commission for his services pursuant to authorization sent by telegraph. The court viewed the matter as turning on what constituted appropriate proof that the telegraph contained contractual authority. The court stated that telegraphic communications were to be treated like other writings, noting that the telegram had to be in written form at each end of the line and that it was appropriate to enter into evidence the original version of the message transmitted, or a copy thereof. *Durkee*, 29 Vt. at 53.
57. 48 N.H. 487 (1869).
59. *Id.* at 411.
61. *Id.*
62. *Id.*
63. *Id.*
64. *Id.*

Many cases are cited . . . from which it is held, that in all controversies between the sender of a message, and the company, the original message is the one left at the office.
plained, "Where a man sends a proposition to another man by tele-
graph and gets a reply accepting the offer, the original message, so far
as binding the acceptor is concerned, is the copy delivered to him at
the other end." 65 The court continued, "The message as communi-
cated to the acceptor and his reply as delivered to the operator to be
returned, are what would govern in construing the contract, provided
both parties voluntarily and of their own accord sent their messages
by the telegraph . . . ." 66 The Howley court concluded:

So when a contract is made by telegraph, which must be in writing
by the statute of frauds, if the parties authorize their agents either in
writing or by parol, to make a proposition on the one side and the
other party accepts it through the telegraph, that constitutes a con-
tract in writing under the statute of frauds. 67

Courts have consistently held that an adequate signature may exist
in telexed or telegraphed documents. 68 In Hessenthaler v. Farzin, 69
the Pennsylvania Superior Court held that a mailgram constituted a
"signed" writing according to the Statute of Frauds. 70 The Penn-
sylvania court noted that the determination of the sufficiency of a
mailgram as a "writing" for Statute of Frauds purposes was one of first
impression for the court. 71 In dicta, the court noted that an increasing
number of questions regarding whether paperless communications
satisfied the Statute of Frauds would likely arise in the future due to
the increasing complexities associated with the business environ-

65. Id.
67. Id.
68. Id.
69. 564 A.2d 990 (1989).
70. Id. at 992 (stating that "the first question we must decide is whether or not the mailgram
appellants sent to Dougherty constitutes a 'signed' writing as contemplated by the [statute of frauds]").
71. Id. The court noted that "[n]either our research nor that of the parties has revealed any
Pennsylvania cases that address the issue of whether or not a mailgram can be sufficient to
satisfy the [statute of frauds]." Id.

The court noted: we should always be satisfied with 'some note or memoranda' that is adequate . . . to
convince the court that there is no serious possibility of consummating fraud by en-
forcement. When the mind of the court has reached such a conviction as that, it neither
promotes justice nor lends respect to the statute to refuse enforcement because of in-
formality in the memorandum or its incompleteness in detail.

Id.
ment. "[T]hese types of questions are likely to arise with greater frequency in the future, as business and individuals increasingly rely on similar methods of negotiation such as electronic mail, telexes and facsimile machines in conducting their business affairs." Hessenthaler forecasted the complex issues that modern businesses must address. As predicted in Hessenthaler, the business and financial sectors have relied on the judicial process to guide them through the turbulence.

A more intrinsic issue regarding the enforceability of telegraphs as contracts under the Statute of Frauds is whether the telegraph is considered "signed." This issue was resolved in Yaggy v. B.V.D. Co. in which the Court of Appeals of North Carolina concluded that printed letters had been held to satisfy the Statute of Frauds; therefore, the type-written name of the seller at the end of the telegram was a sufficient signing so long as the seller directed the affixing of it with the intent to identify the telegram.

The concern in Yaggy involved a civil action to obtain specific performance of a contract to convey land. The plaintiff, Edward Yaggy, offered to purchase the property at issue from the defendant, B.V.D. On the same date that B.V.D. accepted Yaggy's offer, B.V.D. transmitted a telegram to Yaggy stating the following:

ACCEPT OFFER OF $250,000 FOR BVD PROPERTY IN CARRBORO NOCAR SUBJECT TO REACQUISITION FROM MONTVALE REALTY CORP =ALBERT D RADER BVD COMPANY INC BVD COMPANY INC

B.V.D. subsequently breached the contract and advised Yaggy that it would not convey the property to him.

72. Id. at 992 n.3.
73. Id.
74. This reliance on the judicial process to solve the complex issues faced by the business sector resulted in the promulgation of state legislation addressing electronic transactions, and ultimately, E-SIGN.
75. See Robertson, supra note 54, at 798.
77. Id. at 501.
78. Id. at 498. The North Carolina Statute of Frauds provides, in part:

All contracts to sell or convey any lands, tenements or hereditaments, or any interest in or concerning them, . . . shall be void unless said contract, or some memorandum or note thereof, be put in writing and signed by the party to be charged therewith, or by some other person by him thereto lawfully authorized.

79. Yaggy, 173 S.E.2d at 498.
80. Id.
81. Id.
The court specifically addressed the question of "whether a telegram to which the vendor's name has been so affixed may be considered signed by the vendor within the meaning of [North Carolina's] statute." The *Yaggy* court responded affirmatively to this inquiry. The court cited *McCall v. Textiles Indus. Inst.*, stating, "The signing of a paper writing or instrument is the affixing of one's name thereto, with the purpose or intent to identify the paper or instrument, or to give it effect as one's act."

The court noted, "Affixing one's handwritten signature, however, is not the only method by which a paper writing may be considered as being signed within the meaning of the Statute of Frauds." The court, citing the Supreme Court of Arizona in *Bishop v. Norel*, stated the generally recognized principle as follows:

> We are fully satisfied that the general rule is that a writing or memorandum is 'signed' in accordance with the statute of frauds if it is signed by the person to be charged by any of the known modes of impressing a name on paper, namely, by writing, printing, lithographing, or other such mode, provided the same is done with the intention of signing.

In recognizing this generally accepted rule, the *Yaggy* court concluded that "[d]efendant appellant's name affixed to the telegram constituted a signing of the telegram by the defendant within the requirement of the statute of frauds."

b. Telex or Telecopier

The telex machine was the direct result of the evolution of the technology that made the telegraph a palpable element of commercial transactions. The telex "allowed each user to have direct access to every other user with a similar machine, without the need of the tele-

---

82. *Id.* at 501.
83. *Id.*
84. 128 S.E. 349 (N.C. 1925).
85. See *Yaggy*, 173 S.E.2d at 501 (citing *McCall* 128 S.E. at 353).
86. *Id.*
90. *See Robertson*, *supra* note 54, at 800.
The enforceability of contracts formed via telex technology was handed down in *Joseph Denunzio Fruit Co. v. Crane:* [92]

[The court] must take a realistic view of modern business practices, and can probably take judicial notice of the extensive use to which the teletype machine is being used today among business firms, particularly brokers, in the expeditious transmission of typewritten messages. No case in point has been called to the court's attention on this particular point, and a diligent search of the authorities has failed to uncover the status of teletype machine as satisfying the California Statute of Frauds . . . [93]

The *Denunzio* court, even with the absence of applicable case law, concluded that the teletype communications constituted a signed contract within the meaning of the Statute of Frauds. [94]

In *Denunzio*, the United States District Court for the Southern District of California examined what constituted a signature under the Statute of Frauds with respect to teletype machines used to create a contract for the sale of grapes. [95] This case began when Associated Fruit Distributors of California, the alter ego of the defendant Crane, sua sponte and without any prior solicitation, sent a telegram to a food broker with whom it had dealt for several years. The telegram contained an offer to book nine cars of Emperor unclassified grapes or eighteen cars of vineyard-run grade grapes. [96] The offer was made subject to confirmation, and the food broker was directed to wire his answer. [97] The plaintiff made a counter-offer through the food broker. [98] Associated Fruit Distributors rejected the food broker's counteroffer and subsequently submitted a revised offer to the food broker by telegram. [99] In this new offer, Associated Fruit Distributors offered to sell fifteen cars of the Emperor grapes. [100] By teletype message, Joseph Denunzio accepted the offer through the food broker. [101]

---

91. *Id.*
92. 79 F. Supp. 117 (S.D. Cal. 1948).
93. *Id.* at 128-29.
94. *Id.*
95. *Id.* at 127-28. The initial offer by Associated Fruit Distributors of California was to book the cars for storage, packing, and distribution. *Id.* at 122. The counteroffer supplied by Joseph Denunzio stated the desire for a total of four cars, two to be shipped to Louisville and two to be stored. Upon Associated Fruit Distributors' rejection of this counteroffer, they submitted a revised offer whereby Associated offered to sell fifteen cars of the grapes. Joseph Denunzio accepted the offer of Associated Fruit Distributors' offer as to three cars. *Id.* at 122-23.
96. *Id.* at 121-22.
97. *Id.* at 122.
99. *Id.*
100. *Id.* at 123.
101. *Id.*
Associated Fruit Distributors confirmed Denunzio’s acceptance by teletype message. However, Associated Fruit Distributors subsequently repudiated the contract, ironically through teletype message.

The primary inquiry that confronted the district court was whether there was a binding contract as a result of Associated Fruit Distributors' offer and Joseph Denunzio’s acceptance. The court held that a binding contract was present and readily conceded that “these teletype messages do not bear the signature in writing of the party to be charged in the sense that they were not literally signed with pen and ink in the ordinary signature of the sender.”

The court explained the modus operandi of teletype machines as follows:

As the court understands the modus operandi of the teletype machines in modern business practice, particularly in connection with this lawsuit… each [party] had a teletype machine in his office and as the machine was operated in one office, it would type the message or memorandum simultaneously in the other office; each party was readily identifiable and known to the other by the symbols or code letters used.

102. Id. at 123. By telegram, Associated Fruit Distributors stated that Red Lion Packing Company, the shipping company, had repudiated the contract, forcing Joseph Denunzio to purchase cover. Joseph Denunzio made an effort to induce the Associated Fruit Distributors to comply with the contract. “Efforts to obtain compliance by Associated Fruit Distributors of its obligation under the contract having failed, and the date of performance of the contract having passed, Joseph Denunzio purchased three cars of U.S. No. 1 Emperor grapes as soon as they were available, and at the best market price obtainable. The three cars cost Joseph Denunzio exclusive of distribution charges, a total of $14,011, which exceeded the contract price for the three cars previously purchased from the Associated Fruit Distributors by $5,723.50.” Id. at 124. Joseph Denunzio would later attempt recovery by initiating proceedings before the War Food Administrator. Id. at 125.

103. Id. at 121.

104. Id. at 128.

105. Id. The sufficiency of tape recorded transactions has also been analyzed by the courts in an attempt at reconciliation with the Statute of Frauds. The United States District Court of Colorado in Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212 (D. Colo. 1972), held that a tape recording satisfied the signature requirement of the Statute of Frauds when both parties knew they were taping their discussion. The Ellis court concluded that the purpose of the signature requirement was to identify the parties and that a tape recording fulfilled this function. Id. at 1228. Commentators have criticized this argument because it ignores the other purpose of the signature requirement, authenticity. See Houston P. Lowry, Does Computer Stored Data Constitute a Writing for the Purpose of the Statute of Frauds and the Statute of Wills?, 9 Rutgers Computer & Tech. L.J. 93, 101 (1982). The Ellis court should have concluded that the parties intended to authenticate the agreement with the tape recording as well as identify the parties. Id. Many courts agree with the conclusion that tape recordings do not satisfy the Statute of Frauds. In Swink & Co. v. Carroll McEntee & McGinley, Inc., 584 S.W. 2d 393 (Ark. 1979), the Arkansas Supreme Court stated that even if the tape recording was a writing, the recording did not satisfy the Statute of Frauds because it was not signed by the party against whom enforcement was sought. In examining whether the tape recording was “signed,” the question was pri-
Under circumstances analogous to that of modern day e-mail messaging, the court simply concluded that the teletype messages satisfied the Statute of Frauds.\textsuperscript{107}

c. Facsimile

The burgeoning use of fax machines has altered our everyday lives, but it has yet to spark the interest of the courts.\textsuperscript{108} However, case law exists that appears to assume that a facsimile transmission constitutes a "writing."\textsuperscript{109}

The issue of whether a facsimile transmission was sufficiently signed under the Statute of Frauds was addressed separately from its nature as a "writing." In \textit{Parma Tile Mosaic & Marble Co. v. Estate of Short},\textsuperscript{110} the New York Court of Appeals held that "a name . . . is not a signature unless inserted or adopted with an intent, actual or apparent, to authenticate a writing."\textsuperscript{111} The court reasoned that the intent to authenticate cannot result from a mere machine-generated name appearing on the face of a document.\textsuperscript{112} Consequently, the court concluded that the particular fax did not fulfill the "signature" requirement of the Statute of Frauds.\textsuperscript{113} However, "nothing in the opinion suggested that a fax is not a writing or that it could not be signed if it bore some human-generated symbol constituting a signing."\textsuperscript{114}

In \textit{Parma Tile}, the controversy involved an allegedly formed contract for the purchase of tile.\textsuperscript{115} A construction manager, MRLS, was employed to coordinate a certain project, whereby MRLS hired a con-

\textsuperscript{107} Denuzio, 79 F. Supp. at 129.
\textsuperscript{108} See Robertson, supra note 54, at 801.
\textsuperscript{109} Id.
\textsuperscript{110} 663 N.E.2d 633 (App. Ct. N.Y. 1996). "Given the greatly increased use of fax machines in recent years, it is surprising that there are no reported cases deciding whether a fax transmission constitutes a sufficient writing for purposes of the Statute of Frauds." See Robertson, supra note 54, at 801. \textit{But see} Bazak Intl Corp. v. Mast Indus., 535 N.E.2d 633 (N.Y. 1989) (appearing to assume that a fax transmission would satisfy the Statute of Frauds).
\textsuperscript{111} See Parma, 663 N.E.2d at 634-35. The plaintiff failed to demonstrate that the defendant affixed its "signature" to the document sent by facsimile machine sufficient to fulfill the signature requirement. \textit{Id.} at 634.
\textsuperscript{112} Id.
\textsuperscript{113} Id. at 635.
\textsuperscript{114} See Robertson, supra note 54, at 802.
construction company to perform as a subcontractor on the project. The construction company attempted to order tile from Parma Tile Mosaic & Marble Co. (Parma) to fulfill its performance as a subcontractor. Parma refused to deliver the tile unless the construction manager guaranteed payment. By facsimile transmission, the construction manager sent the following message to Parma:

This company would be willing to guarantee payment on regular terms for goods delivered . . . . [Upon delivery of the tile] [y]ou [sic] would then bill Sime Construction for those goods delivered. MRLS would guarantee payment for goods delivered to the Neheimiah Project in the event Sime Construction does not pay within terms . . . . Please consider all of the above in making your decision.

The name of the construction manager, MRLS, was printed across the top of the fax, but it was unsigned. Parma delivered the tile to Sime, and when Sime failed to pay Parma, Parma billed MRLS in reliance on the purported agreement.

In the trial court, Parma argued that the fax constituted an enforceable guarantee because the name of MRLS appeared across the top of the fax and satisfied the signature requirement of the Statute of Frauds. Parma further contended that because MRLS had intentionally programmed its fax machine to print the company name on top of all faxed documents, the signature requirement was satisfied. The trial court agreed with Parma and concluded, "The signature required does not necessarily have to be written in ink at the bottom of the purported guarantee but may include any symbol or signature, whether written, printed or stamped, on any part of the document so long as the intent to be bound is demonstrated."

116. Id. at 1020. Sime Construction Company was the subcontractor employed by MRLS to perform the subcontract work on the project. Sime Construction Company was a codefendant in this action.
117. Id.
118. Id.
119. Id. at 1020.
120. Id.
121. Parma, 663 N.E.2d at 634.
122. Id.
123. Id.
124. See Parma, 590 N.Y.S.2d at 1021. The trial court in Parma granted Parma's motion for summary judgment. Id.
125. Id. at 1020.
However, the Court of Appeals of New York reversed. The court stated, "As former Chief Judge Cardozo has observed, a signature for the Statute of Frauds purposes may be 'a name, written or printed, [but] is not to be reckoned as a signature unless inserted or adopted with an intent, actual or apparent, to authenticate a writing.'" The court addressed the plaintiff's argument by noting that "[p]laintiff contend[ed] that we may infer satisfaction of this require-
ment because the fax machine had been programmed by MRLS to identify each page of the document with 'MRLS Construction.'" The court, therefore, concluded:

The act of identifying and sending a document to a particular desti-
nation does not, by itself, constitute a signing authenticating the contents of the document for the Statute of Frauds purposes and [sic] reject plaintiff's argument that such an inference is warranted here. It is undisputed that MRLS' fax machine, after being programmed to do so, automatically imprinted 'MRLS Construction' on every page transmitted, without regard to the applicability of the Statute of Frauds to a particular document. We also reject plaintiff's contention that the intentional act of programming a fax machine, by itself, sufficiently demonstrates to the recipient the sender's apparent intention to authenticate every document subse-
quently faxed. The intent to authenticate the particular writing at issue must be demonstrated.

The Parma court focused on the U.C.C.'s requirement that for a con-
tract to be signed, there must exist an intent to authenticate the writing. The automatic programming of the fax machine did not demonstrate the requisite intent of the parties to authenticate the writing.

B. Legislative Response to the Statute of Frauds

There has been little opportunity for the courts to adjudicate whether an electronically formed contract satisfies the "writing" and "signature" requirements of the Statute of Frauds. The case law, however, "suggests that courts would find that electronic records can

126. See Parma, 663 N.E.2d at 634 (noting that "plaintiff has failed to demonstrate that MRLS affixed its 'signature' to the documents sent by facsimile machine sufficient to fulfill the subscription

requirement.").
127. Id. at 634-35.
128. Id. at 635.
129. Id.
130. Id.
131. See Szafran, supra note 6, at 494 (noting "[n]o lawsuit has yet been adjudicated that directly examines whether a contract formed via an electronic transmission satisfies the Statute of Frauds. Because of this absence of clear authority, doubt as to whether electronic transactions constitute signed writings persists.").
meet the statutory writing requirements, and that electronic signatures can meet the statutory requirements."\textsuperscript{132} Some argue that to hold otherwise "would be inconsistent with 'commercial experience' in today's fast-paced business environment."\textsuperscript{133}

The most recent case law has supported this proposition, although with some reluctance. In \textit{In re RealNetworks, Inc., Privacy Litigation},\textsuperscript{134} the United States District Court for the Northern District of Illinois held that an electronic agreement authorizing the use of various software packages could satisfy the writing requirements of the Federal Arbitration Act.\textsuperscript{135} Although decided without the guidance of E-SIGN, the court noted that "Congress's then current discussions over E-SIGN address only 'the uncertain legal effect of an electronic record or an electronic signature.'"\textsuperscript{136} The court subsequently concluded that the use of the term "written" in the Federal Arbitration Act envisioned the classification of electronic communications as satisfying the statutory mandate.\textsuperscript{137} The court acted with some reluctance, however, stating that "the Court does not now find that all electronic communications may be considered 'written.'"\textsuperscript{138}

The difficulty in relying on the judiciary to lay down guidelines for the enforceability of electronic contracts is the evident time constraints. Can the business and legal worlds continue to grow at the present pace if they are subject to the continuous legal uncertainty associated with the enforceability and validity of electronic contracts? One commentator argues:

\begin{quote}
Even if the courts should determine that electronic messages are sufficient to satisfy the Statute of Frauds, those determinations would occur on a case-by-case basis over a period of years. Given
\end{quote}

\begin{footnotes}
\footnotetext{132}{See Smedinghoff & Bro, supra note 32, at 735. Therefore, the "concerns over whether electronic records and electronic signatures will satisfy these legal requirements may not be warranted." \textit{Id.} at 734.}
\footnotetext{133}{See Dipaolo, supra note 29, at 155.}
\footnotetext{134}{2000 U.S. Dist. LEXIS 6584 (N.D. Ill. May 10, 2000).}
\footnotetext{136}{\textit{In re RealNetworks, Inc., Privacy Litigation}, 2000 U.S. Dist LEXIS 6584, at *10-11.}
\footnotetext{137}{\textit{Id.} at 355, at 1191.}
\footnotetext{138}{\textit{In re RealNetworks, Inc., Privacy Litigation}, 2000 U.S. Dist. LEXIS 6584, at *8. The reluctance of the RealNetworks court is illustrated by several other cases addressing the formation of electronic contracts. For example,}
\end{footnotes}

\begin{quote}
In \textit{Ballas v. Tedesco}, [41 F. Supp. 2d 531 (D.N.J. 1999)] a federal district court held, "[T]he exchange of e-mails, however, does not satisfy the statutory requirement of a written instrument signed by the Defendants." \textit{Id.} at 541.] Yet, in \textit{Barman v. Union Oil Co.}, [1999 U.S. Dist. LEXIS 13973 (D. Or. Aug. 13, 1999)] another federal district court ruled that "numerous e-mail messages and memoranda" amounted to "other writings constituting a contract." \textit{Id.} at 28.
\end{quote}

\textit{See Hays, supra} note 135, at 1192.
the existing reluctance of parties to engage in electronic commerce, it is unlikely that enough courts would decide that electronic messages satisfy the Statute of Frauds to give much comfort to business persons in the foreseeable future. Therefore, it is essential that legislatures examine the relation of electronic commerce to the Statute of Frauds.\textsuperscript{139}

The state legislatures around the country must have overwhelmingly agreed with the above-noted commentator's argument. A vast majority of states have enacted legislation affecting the Statute of Frauds as it relates to electronic commercial transactions.\textsuperscript{140}

The evident intent behind the states' legislation was to provide the framework by which electronically-formed contracts are equated with their paper counterparts, thereby satisfying the Statute of Frauds. "Although this result is nearly universal, the drafters of this legislation have used different, and sometimes confusing terminology."\textsuperscript{141} "Two models have emerged with respect to whether electronic messages satisfy the Statute of Frauds. One is based on the landmark Utah Digital Signature Act.\textsuperscript{142} The other, which is much broader in scope, is codified in the Illinois Electronic Commerce Security Act.\textsuperscript{143}

1. The Utah Digital Signature Act\textsuperscript{144}

The Utah Digital Signature Act (Utah Act), passed in 1995 and substantially amended in 1996, was the first attempt by a state to amend the provisions of the Statute of Frauds to allow for the enforceability and validity of electronically-formed contracts.\textsuperscript{145} The Utah Act was not an ill-conceived venture, but rather a comprehensive undertaking to "conform the writing and signature requirements of the Statute of Frauds to the needs of electronic commerce."\textsuperscript{146} The Utah Act has also served as model legislation for several states.\textsuperscript{147}

\textsuperscript{139} See Robertson, supra note 54, at 808. The history of the telegraph provides a vivid illustration:

It was forty or fifty years after the invention of the telegraph before a majority of state courts had affirmed that a telegram could be a writing satisfying the Statute of Frauds and, as late as 1979, a state court held that a telegram did not satisfy the Statute of Frauds because it was not signed. See Pike Indus. v. Middlebury Assocs., 398 A.2d 280, 282 (Vt. 1979).

\textsuperscript{140} Id. at 809, n.130.

\textsuperscript{141} Id. at 819.

\textsuperscript{142} Id. at 816.

\textsuperscript{143} 5 ILL. COMP. STAT. 175/5-105 to 175/99-1 (West 1998).

\textsuperscript{144} UTAH CODE ANN. § 46-3-101 to 46-3-504 (1998).

\textsuperscript{145} Id.

\textsuperscript{146} See Robertson, supra note 54, at 819.

\textsuperscript{147} Id.
Under the Utah Act, "digital signatures" laid the foundation for what was the first comprehensive approach to reconcile electronic transactions with the writing and signature requirements of the Statute of Frauds.\textsuperscript{148} Pursuant to the Utah Act, a digitally-signed message satisfies both the "writing" and the "signature" requirements of the Statute of Frauds if the digital signature has been authenticated by reference to the public key listed in a valid certificate issued by a licensed certification authority.\textsuperscript{149} The Utah Act also provides that "[n]othing in this chapter precludes any symbol from being valid as a signature under other applicable law, including [the] Uniform Commercial Code, Subsection 70A-1-201(29)."\textsuperscript{150} Furthermore, "nothing in this Chapter precludes any message, document, or record from being considered written or in writing under other applicable state law."\textsuperscript{151} These provisions, however, do not affirmatively state that any electronic record, other than the one that is digitally signed, can constitute a 'signed writing.' Instead, the Utah Act leaves the issue up to subsequent judicial determination. Accordingly, it is unclear whether an electronic record that is not digitally signed could satisfy the Statute of Frauds requirements in Utah.\textsuperscript{152}

What is clear is that "the 'digital signature model' epitomized by the Utah Act requires the parties in an electronic commerce transaction to use digital signatures to assure that their electronic records will satisfy the Statute of Frauds."\textsuperscript{153}

2. The Illinois Electronic Commerce Security Act\textsuperscript{154}

Unlike the Utah Act, the Illinois Electronic Commerce Security Act (Illinois Act), passed in 1998, takes a broad approach as to how electronic contracts satisfy the signed writing requirement of the Statute of Frauds.\textsuperscript{155} The Illinois Act is "technologically neutral," i.e., it recognizes the legal legitimacy of electronic records and signatures.

\textsuperscript{148} Id.
\textsuperscript{149} Id. at 821.
\textsuperscript{150} Utah Code Ann. § 46-3-401(2) (1998).
\textsuperscript{151} Id. at § 46-3-403(2) (1998).
\textsuperscript{152} See Robertson, supra note 17, at 481. With respect to the issue of authenticity: [T]he Utah Act provides that if the digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority, the court shall presume that the digital signature is that of the person listed in the certificate and that it was affixed by that person with the intention of signing the message.
\textsuperscript{153} Id. at 481-82.
\textsuperscript{154} 5 Ill Comp. Stat. 175/5-105 (West 1998).
\textsuperscript{155} Id.
under the [S]tatute of [F]rauds, regardless of the technology used to create them."\textsuperscript{156}

The Illinois Act clearly equates an “electronic record” with a “writing” and an “electronic signature” with a “signature.”\textsuperscript{157}

Hence, Illinois courts are no longer free to interpret the statute of frauds’ requirements as literally requiring a manual signature in ink on paper. Thus, both businesses and consumers in Illinois can enter into electronic commerce transactions, confident that the transactions will not be subsequently invalidated based solely on the medium the parties used to consummate their transaction.\textsuperscript{158}

In addition, the Illinois Act supplies “workable and broad definitions of the terms ‘electronic record’ and ‘electronic signature.’”\textsuperscript{159} Therefore, the Illinois Act allows parties to an electronic transaction to choose an electronic signature and assures them that whichever method is used will comply with the Statute of Frauds.\textsuperscript{160}

The Illinois Act appears to have satisfied its goal of amending the Statute of Frauds so that electronic records and electronic signatures will comport with the requirements enunciated in the Statute of Frauds. “[T]he Illinois Act removes any doubt about the legal legitimacy of electronic records and electronic signatures.”\textsuperscript{161}

3. \textit{Uniform Electronic Transactions Act}\textsuperscript{162}

In 1996, the National Conference of Commissioners on Uniform State Laws (NCCUSL)\textsuperscript{163} began drafting the Uniform Electronic Transactions Act (UETA).\textsuperscript{164} Three years later, the NCCUSL gave its final approval for the uniform law.\textsuperscript{165} Since its approval, and just prior to when E-SIGN became effective, eighteen states had already adopted the UETA.\textsuperscript{166}

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{156} See Robertson, \textit{supra} note 17, at 486.
\item \textsuperscript{157} 5 ILL. COMP. STAT. 175/5-105 (West 1998).
\item \textsuperscript{158} See Robertson, \textit{supra} note 17, at 487-88.
\item \textsuperscript{159} \textit{Id.} at 488.
\item \textsuperscript{160} \textit{Id.}
\item \textsuperscript{161} \textit{Id.} at 489.
\item \textsuperscript{162} \textit{UNIF. ELECT. TRANSACTIONS ACT} §§ 1-2d, 7A U.L.A. 21 (Supp. 2001).
\item \textsuperscript{163} The National Conference of Commissioners on Uniform State Laws, in conjunction with the American Law Institute, prepare the UETA. The NCCUSL also amends the various uniform laws, including the recently amended Revised Article 9, Secured Transactions.
\item \textsuperscript{164} \textit{UNIF. ELECT. TRANSACTIONS ACT}.
\item \textsuperscript{165} Amelia H. Boss, \textit{UNIFORM ELECTRONIC TRANSACTIONS ACT}, 588 PLI/Pat 391, 393 (2000).
\item \textsuperscript{166} \textit{Id.} at 393. These eighteen states are Arizona, California, Florida, Idaho, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Minnesota, Nebraska, Ohio, Oklahoma, Pennsylvania, South Dakota, Utah, and Virginia. \textit{Id.}
\end{enumerate}
\end{footnotesize}
The UETA directly confronts the validity and enforceability of electronic contracting. The central legal requirements provided under the UETA are set forth in section 7, which expressly validates electronic records, signatures, and contracts. An electronic record or signature may not be denied legal effect or enforceability solely because it is in electronic form. In addition, an electronic contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation. Any record created, generated, sent, communicated, received, or stored by electronic means constitutes a required writing. Any 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 constitutes a signature and satisfies any legal requirements for a signature.

Section 3 of the UETA limits the scope of the uniform law to "transactions," and Section 2 defines "transactions" as "an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs." Therefore, the UETA is expressly limited to the electronic signatures and records relating to a transaction, and does not apply to all writings and signatures. Not only does the UETA limit its applicability to "transactions," but it requires that the parties to the transaction agree to conduct the transaction by electronic means prior to the Act taking effect.


(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law.

Id.

168. Id. at 97.

169. Id.

170. Id.

171. Id. at § 2(7)-(8) at 29.

172. Id. at § 3.


174. See Boss, supra note 165, at 395.

175. See Unif. Elect. Transactions Act at § 5. Section 5 states, in part:

(a) This [Act] does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.

(b) This [Act] applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.

With the advent of globalization and widespread use of the Internet, the United Nations joined the fray of e-commerce regulation. Adopted in 1996 and subsequently amended in 1998, the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (Model Law) sought to directly address the international commercial laws within the framework of cyberspace. The structure and language of the Model Law address the validity and enforceability of electronic contracting for the international, rather than domestic stage.

The Model Law "seeks to place electronic communications on par with the legal treatment accorded to traditional paper-based types of communications." The international scheme applies to information in the form of a data message that is used in the context of commercial activities. The language provides that: (1) information in the form of data messages shall not be denied legal effect, validity, or enforceability on that basis alone; (2) any legal requirements that information be in "writing" will be met by a data message if the information contained therein is accessible so as to be usable for subsequent reference; (3) any legal requirements for "signatures" may be satisfied by data messages; and (4) legal requirements for "original" documents may be met by data messages.

III. The Electronic Signatures in Global and National Commerce Act

The Electronic Signatures in Global and National Commerce Act (E-SIGN) is the federal government's response to the validity and enforceability of electronic contracting in light of the legal uncertainty created by the Statute of Frauds. "Not since notarized written signatures replaced wax and signet rings has history seen such a funda-

---

177. See Overby, supra note 18, at 221.
178. Id. at 222.
179. Id.
180. Id. at 223.
181. Id. at 223.
182. Id. at Art. 5. (1998).
183. Id. at Art. 6.
184. Id. at Art. 7.
mental change in contract law." Since October 2000, electronic contract executions have been accepted as legally binding. "It's not so much a change-the-state-of-the-world law as it is a statement that the government approves of the paperless way of doing business."

E-SIGN is the offspring of two separate bills. In November 1999, the U.S. House of Representatives passed the Electronic Signatures Act, and the U.S. Senate passed the "Millennium Digital Commerce Act." The two bills were reconciled in a congressional conference committee to produce E-SIGN.

A. General Rule: Validity of Electronic Signatures and Contracts

E-SIGN directly addresses the fundamental dilemma posed by the writing and signature requirements of the Statute of Frauds, validating both electronic signatures and electronic contracts as a whole. Section 7001 of the Act validates electronic contracting. A signature, contract, or other record relating to any transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because it is in electronic form. Furthermore, contracts relating to any transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation. "The law is a broad and general statement that contracts cannot be invalidated simply because they are in digital form."

Like the UETA from which most of its definitions are taken, E-SIGN assures that all electronic contracts are treated on par with paper records and paper-based signatures through its broad definitions of "electronic record" and "electronic signature." Any contract or record created, generated, sent, communicated, received, or stored by electronic means constitutes a writing sufficient to satisfy any written

187. Id.
188. Id.
193. Id. at § 7001 (a)(1).
194. Id. at § 7001 (a)(2).
195. See Ballard, supra note 186, at B1.
requirement. Moreover, any 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, will constitute a signature and satisfy any legal requirement for a signature. For purposes of E-SIGN, virtually any electronic means of recording information may be sufficient for an electronic record and nearly any electronic evidence that a party to an electronic contract has acted with the intent to authenticate a record may be an electronic signature.

Unlike various state electronic signature enactments, neither E-SIGN nor the UETA requires the use of specific technologies to assist authentication of the signing party or the integrity of the electronic record itself. Instead of supplying states with a recommended or required verification technology, E-SIGN placed restrictions on the authority of the states to demonstrate a preference for authentication technologies.

Although E-SIGN displaced the prior legislative assertions of the states, the Act did not alter the underlying substantive law. Title I of E-SIGN specifically provides that “[it does not] limit, alter, or otherwise affect any requirement . . . relating to the rights and obligations of persons” that is effectuated through other law, “[except] a requirement that contracts or other records be written, signed, or in non-electronic form.”

197. Id. at § 7006(4).
198. Id. at § 7006(5).
200. A small number of states require the use of a specific technology to make an electronic signature in order to receive legal recognition. See, e.g., Utah Code Ann. § 46-3-201 - 46-3-504 (1998); Ill. Comp. Stat. Ann. 175/5-105 - 175/5-145 (West 2000). A substantially larger number of states passed laws that set forth standards that an electronic signature must meet before being legally recognized. For example, the laws state that digital signatures clearly meet the standard, but then do not refer to a specific technology. These standards usually require that an authentication method be unique to the person using it and be linked to the signed record in such a manner that if the content of the records were changed, the signature will be invalidated. See Witte & Winn, supra note 199, at 298 n.24. See e.g., Alaska Stat. § 09.25.500 - 09.25.520 (Michie 2000); Ky. Rev. Stat. Ann. § 369.010 - 369.030 (Michie 2000); Nebraska Digital Signatures Act, § 86-1701 (1999).
202. Id. at § 7002(a)(2)(A)(i).
203. Wittie & Winn, supra note 199, at 298.
204. Title I contains all the Act’s operative provisions governing the use of electronic signatures and records, except for the special provisions on “transferable records” which are contained in Title II. Title III of E-SIGN contains provisions directing the Secretary of Commerce to promote the validity of electronic signatures and records on an international basis. See Witte & Winn, supra note 199, at 299 n.27. See 15 U.S.C.A. § 7001 (2001).
205. Id. at § 7001(b).
However, E-SIGN does not force electronic records and signatures upon contracting parties; both the use and acceptance of electronic records and signatures is voluntary.\textsuperscript{206} Title I of the Act specifies that the Act “does not require any person to agree to use or accept electronic records or signatures.”\textsuperscript{207} E-SIGN does not require an agreement to incorporate the use of electronic signatures to effectuate their legal validity and enforceability.\textsuperscript{208} E-SIGN’s posture allows the parties to a transaction to choose whether to use or accept the use of electronic signatures and electronic records without requiring the parties to commit to either.\textsuperscript{209} The voluntary requirement is satisfied if a party assents to the use of electronic signatures and records or manifests behavior consistent with acceptance.\textsuperscript{210}

Although E-SIGN maintains a posture of a voluntary agreement of acceptance and use, it explicitly enumerates a summary of the intended goals of the Act by listing the guiding principles for the application to international commerce.\textsuperscript{211} Parties to an electronic transaction are able to “determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced.”\textsuperscript{212} Combining meaningful goals and a broad and voluntary posture, E-SIGN clearly establishes the validity of electronic signatures and electronic records for interstate and international commerce.\textsuperscript{213}

For example, there are no changes to the content or timing of notices or disclosures that must be avoided pursuant to federal or state law in connection with any transaction. To avoid doubt regarding what probably would otherwise have been regarded as a particular application of this rule, the Act also specifies that Title I does not affect the ‘proximity’ required by other law with respect to ‘any warning, notice, disclosure, or other record required to be displayed, or publicly affixed.’ This provision was intended to ensure, for example, that a hazard warning could still be required to be displayed on or near an item, even if it is electronic.

\textit{See} Wittie \& Winn, \textit{supra} note 199, at 299.

\textsuperscript{206} \textit{See} Wittie \& Winn, \textit{supra} note 199, at 299.

\textsuperscript{207} 15 U.S.C.A. § 7001(b)(2) (2001). The Act exempts a governmental agency from the voluntary posture of the Act. Section 7001 (b)(2) states that the Act does not “require any person to agree to use or accept electronic records or signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.” \textit{Id.} at § 7001(b)(2).

\textsuperscript{208} \textit{See} Wittie \& Winn, \textit{supra} note 199, at 299. \textit{See} § 7001(c) of the Act which states the consumer consent requirement. Under this requirement, the Act requires affirmative consent by a consumer to use or accept electronic signatures and records.


\textsuperscript{210} \textit{See} Wittie \& Winn, \textit{supra} note 199, at 299.


\textsuperscript{213} \textit{See} Zoelick, \textit{supra} note 2, at 10.
B. Scope of E-SIGN

E-SIGN's coverage of electronic transactions is intentionally broad, and the foundation of the Act facilitates its broad nature. Congress has recognized that "the promotion of growth in private sector electronic commerce through [f]ederal legislation is in the national interest because that market is globally important to the United States." In order to fulfill its purposes, E-SIGN must encompass both interstate and foreign commerce. Congress stated the following purposes of E-SIGN:

1. Transactions Within the Scope of E-SIGN

The general rule established by E-SIGN is that a contract, signature, or other record related to any transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because it is in electronic form. E-SIGN defines the term transaction as:

---

216. Id. at 2-3.
218. 15 U.S.C.A. § 7001(a)(1) (2001). This is comparable to the provisions under the UETA, which also applies to electronic records and signatures "relating to a transaction," except that the UETA is limited to transactions governed by the relevant state's law, not to those in interstate or foreign commerce. See UETA § 3(a).
An action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct:

(A) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) services, and (iii) any combination thereof; and

(B) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.\(^\text{219}\)

The broad definition of “transaction” is intended to cover business, and consumer and commercial conduct,\(^\text{220}\) including but not limited to the exemplary list enumerated in the Act.\(^\text{221}\) The types of conduct and transactions delineated are intended to be broadly construed and applied.\(^\text{222}\) According to a Senate colloquy between Senators Phil Gramm and Spencer Abraham,\(^\text{223}\) “a unilateral action or set of actions by one of the parties to the underlying transaction, or by any other person with any interest in the underlying transaction, or a response by one party to the other’s action, all are covered by the [A]ct.”\(^\text{224}\) The Senators continued, “[I]t is the nature of the activity, rather than the number of persons or the identity or status of the person or entity involved in the activity, that determines the applicability of the [A]ct.”\(^\text{225}\)

However, the full scope of E-SIGN is established by its use of the phrase “relating to.”\(^\text{226}\) While the definition of “transaction” relates to activity “between two or more persons,” the definition expressly


\(^{220}\) The Act’s definition specifically refers to “consumer” conduct to avoid any possible confusion as to whether business or commercial conduct involving consumers is governed by the Act. The definition of “transaction” in the UETA does not expressly include consumers, but the Official Comments make clear that the language is to be “construed broadly to include commercial and business transactions involving individuals who may qualify as ‘consumers’ under other applicable law.” UETA § 2 cmt. 12. See Witte & Winn, supra note 199, at 319 n.132.

\(^{221}\) “[T]he term ‘including’ is not one of all-embracing definition, but connotes simply an illustrative application of the general principle.” Federal Land Bank of St. Paul v. Bismark Lumber Co., 314 U.S. 95, 100 (1941). “[D]rafts of the definition that were circulated and discussed among congressional staff prior to the final conference report on the Act and that contained more lengthy itemizations of included conduct were rejected so as to avoid any inference that the description was a definitive listing or that omitted items were not included within the definition.” Witte & Winn, supra note 199, at 319.

\(^{222}\) See Witte & Winn, supra note 199, at 319.

\(^{223}\) Senator Phil Gramm (R-TX) and Senator Spencer Abraham (R-MI).

\(^{224}\) See 146 CONG. REC. S5282 (2000).

\(^{225}\) Id. at S5282. The types of activities described in the Act are intended to be broadly interpreted. The legislative history of the Act emphasizes that the reference to “services” is not exclusive to any one type of service, but rather “cover[s] any activity that would qualify as a financial activity, an activity incidental to a financial activity, or a complementary activity . . . .” Id.

\(^{226}\) See Witte & Winn, supra note 199, at 320.
encompasses any action "relating to" such activity.\textsuperscript{227} It is evident, therefore, that E-SIGN extends beyond actual transaction documents to encompass all ancillary records, such as applications, filings, notices, and similar documentation.\textsuperscript{228} The dispositive inquiry of whether a record or signature is covered by E-SIGN is whether that record or signature bears a sufficient relationship to the activities of business, consumer, or commercial affairs.\textsuperscript{229}

2. \textit{Transactions Specifically Excluded from E-SIGN}

In response to administrative and consumer concerns over the effect of E-SIGN on certain transactions, Congress included several express restrictions on its applicability.\textsuperscript{230} Pursuant to section 7003, the operative provisions under section 7001 shall not apply to a contract or other record to the extent that it is governed by:

\begin{itemize}
  \item[(1)] a statute, regulation, or other rule of law governing the creation and execution of wills, codicils, or testamentary trusts;
  \item[(2)] a State statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; or
  \item[(3)] the Uniform Commercial Code, as in effect in any State, other than sections 1-107 and 1-206 and Articles 2 and 2A.\textsuperscript{231}
\end{itemize}

The consequence of these specific exclusions from the coverage of E-SIGN is simply the recognition of the foundation that has supported contractual formation and execution.\textsuperscript{232} Furthermore, the exclusions illustrate those areas in which an arms length arrangement and execution of an agreement is essential to the protection of all interests involved, namely wills and issues of family law.\textsuperscript{233}

\textsuperscript{227} Id. at 319. For example, forms that are completed to open a customer account with a retail business, a bank, or a brokerage firm, as well as documents needed in order for an investor to open an individual retirement account (IRA) or 401(k) plan are related to the business, savings, or investment transactions that will occur under that account or plan and are within the coverage of the Act.

\textit{Id.}

\textsuperscript{228} Id.

\textsuperscript{229} Id. at 321.


\textsuperscript{232} Congress has thus recognized that in several contexts, electronic signatures and agreements are not sufficient to afford the protection otherwise obtainable through the application of the Statute of Frauds.

\textsuperscript{233} E-SIGN explicitly provides for review of the exceptions. \textit{See} E-SIGN at § 7003(c). The Secretary of Commerce will review the exceptions of subparts (a) and (b) in 2003 to ascertain
3. Consumer Consent

The central tenet of E-SIGN is the validation that it confers upon electronic signatures and electronic records. E-SIGN, however, does not require the use or the acceptance of the electronic medium. It provides consumers with supplemental protection.

E-SIGN contains a carefully scripted “opt-in” provision precluding any assumption of consent on the part of consumers absent the fulfillment of certain prerequisites. Under section 7001(c)(1), an electronic record may be substituted for a record that is otherwise required to be in writing only if:

1) the consumer has affirmatively consented to such use and has not withdrawn such consent, [and]
2) the consumer, prior to consenting, is provided with a clear and conspicuous statement informing the consumer of any right or option of the consumer to have the record provided or made available on paper or in non-electronic form, and the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form (which may include termination of the parties’ relationships), or fees in the event of withdrawal of consent.

The consumer’s consent must be electronic or confirmed electronically “in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent.”

E-SIGN, however, provides consumers with an avenue to withdraw their consent to receiving electronically-generated records. Although its defense of the consumer is noteworthy, the Act does not fail to protect those that have acted in reliance on the consumer’s consent. Section 7001(c)(4) provides, “Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer . . . prior to implementation of the consumer’s withdrawal of the consent.”

whether the continuation of the exceptions is beneficial to the protection of consumers. Id. at (c)(1).

235. Id. at § 7001(b)(2).
236. Id. at § 7006(1). This section defines “consumer” as “an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual.” Id.
consent." E-SIGN strives for one thing: the legal validity and enforceability of electronically executed contracts. Its goal will not be thwarted by the withdrawal of consent after the execution of the electronic documents.

4. Transactions in Foreign Commerce

E-SIGN not only governs transactions in or affecting domestic commerce, but it also seeks to promote and facilitate the recognition of electronic signatures and electronic records by the international community. Title III enumerates specific objectives to be promoted in the international electronic commerce arena:

1) Removing paper-based obstacles to electronic transactions by adopting into account the enabling provisions of the Model Law on Electronic Commerce adopted in 1996 by the United Nations Committee on International Trade Law (UNCITRAL);
2) Permitting the parties to a transaction to choose the technology of their choice when entering into an electronic transaction, with assurance that their selected technologies and implementation models will be recognized and enforced;
3) Affording the parties to a transaction the opportunity to prove in a court or other proceeding that their authentication approaches and transactions are valid; and
4) Adopting a nondiscriminatory approach to electronic signatures and authentication methods of other jurisdictions.

Congress further recognized the need for coverage with respect to international commerce. The Senate noted the following:

Increasingly, online transactions are not just interstate but international in nature and this creates a clear need for international recognition of electronic signatures and records that will not create barriers to international trade. [E-SIGN] directs the Secretary of Commerce to take an active role in bilateral and multilateral talks to promote the use and acceptance of electronic signatures and electronic records worldwide.

E-SIGN, unlike other forms of electronic signature legislation, has recognized the value to the business and financial sector in promoting international "paperless" transactions. While traditional contract formation and execution may have constituted a barrier to international transactions, E-SIGN facilitates their expansion.

244. Id. at § 7001(a).
245. See Perkins, supra note 230, at 6.
246. Id.
247. 146 CONG. REC. S5288 (2000).
E-SIGN’s greatest influence may be its preemptive ability. The Act clearly promotes uniformity among states, in particular by promoting the UETA. Section 7002 provides that E-SIGN will supersede all state law that is inconsistent with it, excepting any state that enacts the UETA or maintains “technological neutrality” by not requiring authentication or implementation technology in order to satisfy the legal validity of the electronic transaction.

With the obvious intent to create harmonization among the states in the name of protecting interstate commerce pursuant to the Commerce Clause, E-SIGN treads an extenuated line between protection of commerce and the principles of federalism. The states have taken great strides in combating the legal uncertainty that surrounds the writing and signature requirements of the Statute of Frauds by enacting legislation to amend the U.C.C. “[I]t’s not a far reach to suspect that some state may challenge the constitutionality of a federal law that, in effect, imposes the federal will on the traditional state prerogatives to set standards and interpret contract law locally.”

Although E-SIGN governs all transactions in or affecting interstate and foreign commerce, the legislation provides that states have authority to “modify, limit or supersede” the provisions of section 101 with respect to state law. States may exercise this authority only by adopting:

[A statute, regulation, or rule of law] (1) that constitutes an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999, except that any exception to the scope of such Act enacted by a State under section 3(b)(4) of such Act shall be preempted to the extent such exception is inconsistent with [E-SIGN];

(2) [such State statute, regulation, or rule of law] specifies the alternate procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records.
if (i) such alternative procedures or requirements are consistent with [E-SIGN]; and (ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.255

The State legislation that may supersede E-SIGN will likely encompass laws adopted before and after the enactment of E-SIGN.256 Superseding state laws, other than the UETA, that are enacted after June 30, 2000, however, must make specific reference to E-SIGN.257 The Act, therefore, prescribes specific conditions under which a state,

255. Id. at § 7002(a)(1)-(a)(2)(A)(i)-(ii). The official version of the UETA contemplated that a state could insert in section 3(b)(4) a list of any existing state laws that the state wanted to exclude from the UETA’s coverage. Section 102(a)(1) of the Act specifies that any laws that are so excepted from the UETA will need to satisfy the Act’s requirements for other superseding state laws under the Act. Id. at § 7002(a)(1). Preemption was a controversial issue during the legislative process.

A third, highly controversial issue debated during the legislative process was the extent to which the E-Sign Act should preempt state law. Since the principal purpose of the legislation is to establish nationwide validity for electronic signatures and records, some level of federal preemption was assumed, but whether that preemption would extend only to directly conflicting state laws or more broadly was a matter of keen contention. In general, the business community argued in favor of the broadest form of preemption, while representatives of the states, including the National Association of Attorneys General, generally demanded limited preemption, claiming that states should continue to have the right to limit the use of electronic methods in business transactions in specific contexts, including contexts that might not be foreseeable at this time. The resolution of this issue centered primarily on language tying the substantive standards of the E-Sign Act to those of the Uniform Electronic Transaction Act (UETA), a model state law adopted by the National Conference of Commissioners on Uniform State Law (NCCUSL) in July 1999. Both the business community and consumers generally approve of UETA’s terms, and members of Congress agreed that the federal legislation should effectively endorse those terms. Whether states should be able to retain autonomy in the details of implementing UETA, however, or whether they should be strictly limited to UETA’s provisions as endorsed by the E-Sign Act, was an extremely divisive issue. As ultimately enacted, the E-Sign Act represents a compromise on this point, providing for preemption only of state laws that vary in significant degree from UETA and its principles as incorporated in the federal statute.

Perkins, supra note 230, at 2. See also Id. at 4. (“The inclusion of the phrase ‘or accord greater legal status or effect to’ in this provision is intended to prevent a state from according a benefit or imposing a burden based on the use of one particular technology or technical specification.”).

256. See Perkins, supra note 230, at 4.

257. See Wittie & Winn, supra note 199, at 324. “Express preemption occurs where Congress has considered the issue of preemption, has included in the legislation under consideration a provision expressly addressing that issue, and has explicitly provided therein that state law is preemted.” Wash. Mut. Band, FA v. Super. Ct. of Los Angeles County, 89 Cal. Rptr. 2d 560, 567 (Cal. Ct. App. 1999). Preemption of state law by a federal statute “may be either express or implied, and is ‘compelled whether Congress’ command is explicitly stated in the statute’s language or implicitly contained in its structure and purpose.” Metro. Life Ins. Co. v. Commonwealth of Mass., 471 U.S. 724, 738 (1985) (citations omitted).
if it so chooses, may preserve its own existing or future statutes, regulations, or other rules of law addressing the validity and enforceability of electronic records and electronic signatures.\(^\text{258}\) E-SIGN thus preempts state law utilizing an unusual form of limited, express preemption.\(^\text{259}\) E-SIGN’s method of preemption is as follows:

Instead of providing, as is more common, that the Act preempts “inconsistent” state laws or simply allowing the preemption of inconsistent state laws to be an implicit result of the supremacy clause of the Constitution, E-SIGN approaches the subject from the opposite direction, setting forth the limited circumstances in which state laws will not be preempted. This is necessitated by the fact that, while E-SIGN clearly does not preempt the field, thereby precluding states from legislating in the area of electronic records and signatures, it also does not limit its preemption to those state laws that are “inconsistent” with the Act. Instead, E-SIGN section 102(a)(1) explicitly does not preempt the 1999 official version of UETA (official UETA), irrespective of any inconsistency between that uniform statute and the Act, while E-SIGN section 102(a)(2) requires all other laws to comply with two standards: consistency with E-SIGN and technical neutrality.\(^\text{260}\)

Although the UETA and E-SIGN differ, E-SIGN supersedes many provisions of the UETA that would otherwise impede the central goal of uniformity that underlies the Act.\(^\text{261}\) For example:

Section 3(b)(4) of the UETA permits states to exclude by exemption specified state statutes from the benefits of the UETA. A good example of a state using this discretionary authority is California, which exempted approximately 65 statutes. Significantly, [the Elec-

\(^{258}\) See Wittie & Winn, supra note 199, at 325. See, e.g., Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338, § 507(a) (1999) (to be codified at 15 U.S.C. § 6807(a) (Supp. 1999)) (noting that the privacy provisions of Title V of the Gramm-Leach-Bliley Act “shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this sub-chapter, and then only to the extent of the inconsistency”); Real Estate Settlement Procedures Act of 1974 (RESPA), 12 U.S.C. § 2616 (1994) (stating that RESPA “does not annul, alter or affect ... the laws of any State with respect to settlement practices, except to the extent that those laws are inconsistent with any provision of [RESPA], and then only to the extent of the inconsistency”); Federal Debt Collection Procedure Act, 28 U.S.C. § 3003(d) (“This chapter shall preempt State law to the extent such law is inconsistent with a provision of this chapter.”). U.S. CONST. art. VI, cl. 2. “[S]ince our decision in McCulloch v. Maryland, it has been settled that state law that conflicts with federal law is ‘without effect.’” Cipollone v. Liggett Group Inc., 505 U.S. 504, 516 (1992), citing Maryland v. Louisiana, 451 U.S. 725, 746 (1981) (citations omitted). “In the absence of an express congressional command, state law is pre-empted if that law actually conflicts with federal law or if federal law so thoroughly occupies a legislative field ‘as to make reasonable the inference that Congress left no room for the States to supplement it.’” Cipollone, 505 U.S. at 516 (citations omitted).

\(^{259}\) See Wittie & Winn, supra note 199, at 324.

\(^{260}\) Id. at 324-25.

\(^{261}\) See Buckley & Tank, supra note 237, at 120.
IV. ANALYSIS

The uncertainty surrounding the enforceability of electronic contracts and signatures perpetuated by the various legislative enactments of the states, coupled with the development of the UETA, precipitated the creation of a preemptive and uniform law addressing the complexities of electronic contracts and signatures. E-SIGN has established a means by which the commercial and business sectors can achieve a level of confidence necessary to utilize electronic transactions with greater frequency. The technology necessary for the use of electronic contracts and signatures will not be curtailed because E-SIGN explicitly remains technologically neutral, thereby facilitating the growth of new digital technologies.

A. Harmonization of Electronic Contract Legislation

The reason for enacting the Electronic Signatures in Global and National Commerce Act (E-SIGN) was the clear lack of uniformity between state legislation, the UETA, and UNCITRAL’s Model Law. As a result of the legislative initiatives, four models of validating electronic contracts have developed. E-SIGN has incorporated these models into a uniform foundation of electronic contracting law through its preemptive provisions.

1. The Digital Signature Model

The Digital Signature Model is epitomized in the Utah Digital Signature Act (Utah Act). The Utah Act was the first comprehensive attempt to validate electronic signatures and records by a state legisla-
ture to modify the state’s Statute of Frauds to accommodate electronic commerce transactions.\footnote{268}{See Robertson, supra note 17, at 482.}


This model does not focus on the attributes that an electronic signature must possess in order to be enforceable as a signature, but rather on the technology used to create the signature itself.\footnote{270}{Id. at 487.} Under the Utah Act, a digitally authenticated communication satisfies both the writing and signature requirements of the Statute of Frauds if the digital signature has been verified by reference to the public key listed in a valid certificate pursuant to an issuance by a licensed certification authority.\footnote{271}{Id. at 481. See Utah Code Ann. § 46-3-401(2) - 403(2).} The Utah Act, however, does provide:

> [N]othing in this chapter precludes any symbol from being valid as a signature under other applicable law, including [the] Uniform Commercial Code . . . nothing in this chapter precludes any message, document, or record from being considered written or in writing under other applicable state law.\footnote{272}{Id. at 482.}

2. The “Proto-Digital Signature Model”

The Proto-Digital Signature Model is very similar to the Digital Signature Model, yet it differs in several crucial respects.\footnote{273}{See also Robertson, supra note 54, at 432.} The legislation enacted pursuant to this model purports to be “technologically neutral” because the legislation does not specify that only digital signature technology will satisfy the Statute of Frauds’ requirements.\footnote{274}{Id.}

The language of these statutes, in effect, limits the authentication procedures to those involving digital signatures or other electronically encrypted devices.\footnote{275}{Id. at 482.} These legislative enactments narrowly define “electronic signatures,” restricting the term’s denotation to a signature
that is “unique to the person using it, . . . and is linked to data [in the electronic record] in such a manner that if the data are changed the electronic signature is invalidated.” 276 In effect:

[T]hese requirements limit the qualifying signatures to digital signatures or other forms of electronic signatures that involves encrypting the underlying message, as these are the only technologies that would satisfy the last criterion. However, these statutes do not provide for any presumptions of authenticity flowing from the use of these reliable forms of electronic signatures. 277

3. The Minimalist Model

The “Minimalist Model” of electronic commerce reform legislation is almost the exact opposite of the Digital Signature Model. 278 Florida’s Electronic Signature Act is truly “technologically neutral” because the statute allows any electronic signature or electronic record to satisfy the Statute of Frauds’ requirements without establishing guidelines as to which technologies are necessary for authentication. 279

The Florida statute defines an electronic signature as “any letters, characters, or symbols, manifested by electronic or other means, executed or adopted by a party with an intent to authenticate a writing,” 280 and it defines “writing” to include “information which is created or stored in any electronic medium and is retrievable in per-

276. See Robertson, supra note 17, at 482.
277. Id.
278. Id. at 483. The legislation differs from the proto-digital model which purports not to specify any particular technology, but which contains stringent requirements of reliability which presently can only be met by digital signatures or other form of encryption. Id. at n.59.
279. Id. at 483.

Thus, the Florida Act did not limit its validation of electronic messages or signatures to ones that were accompanied by a digital signature or that had any other particular indicia of reliability. The Florida legislature apparently did not see any need to provide for any technology-based solution to the problems of record integrity or signer authentication. Presumably, existing Florida evidentiary law would be sufficient to deal with these issues. Thus, the ‘minimalist model’ of electronic commerce reform legislation is almost exactly the opposite of the digital signature model. The minimalist model is truly ‘technology neutral,’ i.e., it does not require the use of any technology to insure that an electronic record satisfies the requirements of the statute of frauds. It also does not create any evidentiary rules for very reliable electronic records or signatures to deal with the dangers posed by the problems of record integrity and signer authentication.

Id. See Id. at 483 (“The statute contained no provisions about either record integrity or signer authentication and made only passing reference to digital signatures.”). The statute gave the Secretary of State the power to issue “certificates for the purpose of verifying digital signatures,” but also provided that no public or private entity was required to participate in the Secretary of State’s certification program. Fla. Stat. Ann. at § 282.74 (West 1999).
The Florida Act provides that "[u]nless otherwise provided by law, an electronic signature may be used to sign a writing and shall have the same force and effect as a written signature."282

However, the Minimalist Model has several shortcomings.283 For example:

First, statutes like the one in Florida make no provision for evidentiary issues at all. This is a serious matter, because even if an electronic record or signature might satisfy the statute of frauds, it is little comfort to a litigant if the state continues to adhere to the "best evidence rule" requiring the production of an "original" writing. In the context of electronic records, there is really no such thing as an "original" . . .

Second, minimalist statutes make no distinction between ordinary electronic records and electronic records which have enhanced evidence of authenticity due to the use of a reliable security procedure in creating or verifying the record . . . .

Third, minimalist statutes make no provision for the voluntary use of digital signatures by the parties. If the parties choose to utilize digital signatures, it is necessary for some fundamental matters about the certification authorities, certificates, etc., to be spelled out in legislation.284

4. The Uniform Electronic Transactions Act Model

The broadest of all the electronic contracting models, the UETA model is truly "technologically neutral"; it recognizes the legal legitimacy of electronic records and signatures under the Statute of Frauds, regardless of the technology used to create them.285 E-SIGN appears to follow this model in its quest for uniformity among electronic contracting legislative initiatives.286

The UETA broadly defines both "electronic record" and "electronic signature."287 The foundation of the UETA's technological neutrality, however, lies in its definition of "electronic": "'Electronic' means relating to technology having electrical, digital, magnetic, wire-
less, optical, electromagnetic, or similar capabilities.” The term is intended to assure that the UETA will continue to apply as new technologies develop. The drafters of the UETA recognized that although the term “electronic” does not cover those technologies that are technically electronic, the term “electronic” was the most descriptive term to sufficiently encompass a substantial majority of contemporary technologies.

The UETA, unlike E-SIGN, specifically addresses the issues of security with respect to electronic signatures and records. While recognizing the inherent liability concerns of electronic contracting, the UETA provides that an electronic message is attributable to an individual if it was an act of the individual. The act of such person may be demonstrated in any manner, including “a showing of efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.”

B. Uniformity Created by E-SIGN’s Express Preemptive Ability

Because the Internet is a borderless medium, it cannot efficiently accommodate a myriad of state legislation with respect to the validity and enforceability of electronic records and signatures. E-SIGN

---

288. See UETA § 2.
289. UETA § 2, cmt. 4. In elaborating on the definition of “electronic,” the drafters of the UETA stated:

The basic nature of most current technologies and the need for a recognized, single term warrants the use of ‘electronic’ as the defined term. The definition is designed to assure that the Act will be applied broadly as new technologies develop. The term must be construed broadly in light of developing technologies in order to fulfill the purpose of this Act to validate commercial transactions regardless of the medium used by the parties.

Id.
290. Id.
291. See UETA at § 2:

‘Security procedure’ means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

Id. See also Id. at cmt. 11.
292. Id. at § 9(a). Under subsection (a), “[S]o long as the electronic record or electronic signature resulted from a person’s action it will be attributed to that person—the legal effect of that attribution is addressed in subsection (b).” Id. at cmt. 1.

Subsection (b) states: “The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties’ agreement, if any, and otherwise as provided by law.” Id.
293. Id. at § 9(a).
294. See Buckley & Tank, supra note 237, at 119.
creates the necessary harmonization in electronic contracting legislation simply through its preemptive ability. The scope of E-SIGN is sufficient to reach all interstate and foreign electronic transactions.\textsuperscript{295} E-SIGN explicitly states that it will supersede all state legislation that does not constitute an enactment of the UETA.\textsuperscript{296} This preemptive ability provides uniformity and promotes the UETA through the express language of the Act.\textsuperscript{297} The power to preempt state law, when exercised by the federal government, is a fundamental pillar to our constitutional foundation.\textsuperscript{298}

The federal power of preemption derives simply from the application of the Supremacy Clause of the U.S. Constitution to congressional legislation, enacted pursuant to the powers granted Congress, that conflicts with state laws. Preemption may be express or implied. Express preemption occurs when Congress explicitly provides in a statute that federal law will supersede, limit, alter, or otherwise override state laws. Implied preemption may arise through congressional occupation of a field of law or through conflict between state and federal law. Implied preemption through occupation of a field may be found when federal law is "so pervasive as to make reasonable the inference that Congress left no room for the States to supplement it" or when "the federal interest is so dominant that the federal system will be assumed to preclude enforcement of state laws on the same subject." If Congress has neither expressly preempted state law nor occupied the field of legislation, courts will find state law preempted to the extent that state and federal law conflict. Conflict may be found either where compliance with both federal and state law constitutes an impossibility, or where state law frustrates the purpose of a federal enactment . . . .

Whether express or implied, when determining whether federal law preempts a particular state law, congressional intent serves as the "ultimate touchstone" of preemption analysis." However, courts will "assume Congress does not exercise lightly." In fields of law traditionally regulated by the states, there is a presumption against preemption unless Congress's intent is unclear or unambiguous.\textsuperscript{299}

Has Congress gone too far with the preemptive nature of the Act? Traditionally, contract law is a province of the states, which are viewed as "laboratories of experimentation."\textsuperscript{300} The states that have made a

\textsuperscript{296} Id. at 7002.
\textsuperscript{297} Id.
\textsuperscript{299} Id. at 391-93.
\textsuperscript{300} See Maureen A. O'Rourke, Progressing Towards A Uniform Commercial Code For Electronic Commerce or Racing Towards Nonuniformity?, 14 BERKELEY TECH. L.J. 635, 641 (1999).
conscious effort to enact legislation to combat the difficulties inherent in the Statute of Frauds have sought to address the needs of their citizens and businesses. E-SIGN clearly supersedes most, if not all, the efforts of the states to solve the problem of validation and enforcement of electronic contracts.  

It has been argued, "[T]he best legal system for electronic commerce will result from continuing experimentation by individual jurisdictions." Likewise, legal scholar Lawrence M. Friedman has identified numerous instances in which state legislation has been used to facilitate and promote economic growth. E-SIGN forces states to act under the auspices of federal contract law, which stifles the states’ abilities to facilitate economic growth. It is "not a far reach to suspect that some state may challenge the constitutionality of a federal law that, in effect, imposes the federal will on the traditional state prerogative to set standards and interpret contract law locally."  

But is the federalism argument for nought? Does the federal government not possess the power under the Commerce Clause to legislate that which effects interstate commerce? Some believe the federal government must act to ensure uniformity in electronic commerce reform legislation to prevent undue disruption or interference with interstate commerce.

1. Preemption and the Uniform Electronic Transactions Act (UETA)

E-SIGN provides:

A State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of [the Act] with respect to State law only if such statute, regulation, or rule of law (1) constitutes an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment . . . by the National Conference of Commissioners on Uniform State Laws in 1999. E-SIGN, therefore, does not preempt the official version of the UETA. It is evident from the congressional objectives of the Act that Congress wanted to create uniformity in the field of electronic records and signatures, minimizing the impediments to the future

302. See Robertson, supra note 17, at 509.
304. See Ballard, supra note 186, at 2.
305. See Tomaszewski, supra note 45, at 439.
306. See Robertson, supra note 17 at 508.
growth of electronic commerce. In addition, Congress desired a limitation on federal authority to preempt state law, and therefore it encouraged state adoption of the official version of the UETA. Consequently, E-SIGN provides states with the authority to "modify, limit or supersede" the Act through the adoption of the UETA. A cursory examination of congressional analysis provides the understanding for their objectives:

Since the text of official UETA was a known quantity, Congress could be comfortable that its adoption would not undermine [the Act's] central purposes or rules. Moreover, if all states were to adopt the official version of UETA, there would still be a uniform, national rule that, while different from [the Act] in various respects, would have substantially similar core provisions. Taken together, these factors made the prospect of a state superseding [the Act's] provisions through the official version of the UETA acceptable to Congress.

On the other hand, Congress was skeptical of whether other state legislative enactments, including any variations of the UETA adopted by states, would conform with E-SIGN's general provisions with respect to the validity and enforceability of electronic records and signatures, and result in the uniformity that Congress desired for the electronic commerce field. Accordingly, the second part of E-SIGN's pre-emption provision, which is applicable to any state law other than the official version of the UETA, is expressly limited by a consistency

310. See 146 CONG. REC. S5224 (daily ed. June 15, 2000) (statement of Sen. Spencer Abraham) "[T]he central purpose of this legislation is to establish a nation-wide baseline for the legal certainty of electronic signatures and records." Id. "I believe that the eventual adoption of UETA by all 50 states in a manner consistent with the version reported by NCCUSL will provide the same national uniformity which is established in the Federal legislation." Id.
311. See Wittie & Winn, supra note 199, at 325.
312. Id.
313. Id. at 326.
314. 15 U.S.C.A. § 7002. Exemption to preemption:
(a) In general. A State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of § 7001 of this title with respect to State law only if such statute, regulation, or rule of law—(1) constitutes an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999, except that any exception to the scope of such Act enacted by a State under section 3(b)(4) of such Act shall be preempted to the extent such exception is inconsistent with this subchapter of subchapter II of this chapter, or would not be permitted under paragraph (2)(A)(ii) of this subsection; or (2) (A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contacts or other records, if (i) such alternative procedures or requirements are consistent with this subchapter and subchapter II of this chapter; and (ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the imple-
standard prohibiting the alteration or complete change of any of E-SIGN’s provisions.\textsuperscript{315}

Because the realm of paperless transactions, specifically electronic transactions on the Internet, is a borderless medium, it cannot efficiently accommodate a patchwork of state legislation regarding the validity and enforceability of electronic signatures and records.\textsuperscript{316} Historically, the formation and execution of contracts has been governed by an intricate web of state legislation.\textsuperscript{317} As noted above, this web of state models can complicate the emergence of an evolving method of contract formation and execution; however, E-SIGN appears to resist specifically addressing the complexities created by the myriad of state legislation, and instead focuses its attention on the tradition of uniformity generated by the UETA.\textsuperscript{318}

E-SIGN supplies its preemptive force through an applicable “consistency standard.”\textsuperscript{319} This standard, however, may lead to confusion:

The semantics of the consistency standard in E-SIGN section 7002 (a)(2)(A)(i) are confusing since they present a seeming paradox of state law that “may modify, limit or supersede” E-SIGN only if it is “consistent” with it. This apparent conflict is resolved, however, by understanding that E-SIGN does not preempt the field; it governs what it addresses, and (except with respect to official UETA) it preempts state law with respect to those matters, but no more. Thus, properly read, the consistency standard prevents any state law (other than official UETA) from either adding to or subtracting from the requirements that E-SIGN imposes.\textsuperscript{320}

\textsuperscript{315} Id. at §7002 (2)(A)(i). The Act specifies that the rules applying to such other laws also apply to laws that are excepted pursuant to the UETA § 3(b)(4), even though such exceptions could be viewed as part of the official version of the UETA. \textit{Id.}

\textsuperscript{316} See O’Rourke, \textit{supra} note 300, at 643.

\textsuperscript{317} Id. at 7002 (a)(2)(A)(i).

\textsuperscript{318} 15 U.S.C.A. § 7002.

\textsuperscript{319} Id. at 7002 (a)(2)(A)(i).

\textsuperscript{320} See Wittie & Winn, \textit{supra} note 199, at 326. For example:

[A] state could not provide that only certain types of electronic records may be considered legally effective or used to satisfy a writing requirement because to do so would be inconsistent with E-SIGN’s base validity rule.

Similarly, a state may not adopt its own, non-conforming consumer consent requirements. E-SIGN section 101(c)(1) provides that the use of an electronic record in compliance with the conditions set forth in that subsection “satisfies the requirement” that the information contained in the record be provided to a consumer in writing. Hence, it is plain that a state law that imposed still more conditions on satisfying that requirement would be inconsistent with section 101(c)(1) and, therefore, would be preempted.
Therefore, E-SIGN affords a state the choice to either adopt E-SIGN or adopt the official UETA. If a state chooses not to adopt the official UETA or adopts a nonconforming version, the state may not adopt any legislation that is inconsistent with the provisions of E-SIGN.321

With respect to states adopting the UETA in its unamended, official form, pursuant to section 7002 (a)(1) of E-SIGN, in matters governed by state law “all of the provisions of UETA will be given effect . . . irrespective of whether those provisions can be viewed as ‘inconsistent’ with E-SIGN.”322

---

For the same reason, a state law (other than official UETA) that imposed fewer or merely different conditions would also be preempted.

Id. Moreover:

[Under E-SIGN’s technical neutrality provisions, a state law could not provide for a presumption of authenticity or give other legal advantages to electronic records or signatures based on the fact that they result form use of a particular technology. This is likely to prevent special legal status being accorded, for example, to PKI or other specific types of security systems. Nothing in E-SIGN, however, prevents private parties from using or requiring that their counterparts use such technologies, based on their own views that the are useful.]

See Wittie & Winn, supra note 199, at n.172.


322. See Wittie and Winn, supra note 199, at 327. For example:

While UETA would not displace, with respect to state law, a provision in E-SIGN section 101 that is not modified, limited, or superseded by a provision of UETA, virtually all the provisions within E-SIGN section 101 are taken from, or address, matters that are directly addressed by UETA and, thus, would be superseded . . . . The fact that E-SIGN provides that a state ‘may’ modify, limit, or supersede E-SIGN by adopting UETA does not mean that a state has the option to adopt official UETA but decide separately whether it wants some or all of the UETA provisions to supersede related provisions in E-SIGN. The state’s choice lies in adopting or not adopting (or in the case of pre-existing laws, choosing whether to repeal or amend) provisions of law that by their nature ‘modify, limit, or supersede.’ A conclusion to the contrary would lead to enormous confusion. Id. at 327 n.173.

A crucial difference between UETA and E-SIGN is the consumer consent provisions in E-SIGN’s section 7001(c):

[The Act provides that a consent conforming with its requirements must be obtained in order to satisfy the writing requirement inherent in any law requiring that information be provided or made available to consumers in writing. UETA, in contrast, provides that, if a law requires information to be provided, sent, or delivered in writing to any person (whether or not that person is a consumer), that requirement is satisfied if the information is provided, sent, or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt. Both E-SIGN and UETA expressly allow parties to provide electronic records to satisfy writing requirements imposed in connection with the provision of information to consumers (and in the case of UETA any other person). Since the UETA provision does so without requiring the type of affirmative consent and related disclosure required by E-SIGN, that provision clearly modifies or supersedes the E-SIGN provision. As a result, in states that adopt the official version of UETA the E-SIGN consumer consent would not be required with respect to information that state law requires to be provided.

See Wittie & Winn, supra note 199, at 327.]
In states adopting non-conforming versions of the UETA, E-SIGN preempts this legislation when it is "inconsistent" with the provisions of E-SIGN. For example, the legislative history of E-SIGN enunciated the requirements of a state seeking to be covered by E-SIGN in section 7002(a)(i):

[A state seeking to be covered by E-SIGN section 7002 (a)(i) is] required to enact or adopt UETA without amendment. Any variation or derivation [sic] from the exact UETA document reported and recommended for enactment by NCCUSL shall not qualify under subsection [(a)] (1) . . . [and] may or may not be eligible [i.e., permitted] under subsection [(a)] (2) . . . . Thus, a State that enacted a modified version of UETA would not be preempted to the extent that the enactment or adoption . . . met the conditions imposed in subsection (a)(2). A state, however, in light of adopting a conforming version of the UETA, may usurp the preemption power of E-SIGN by adopting E-SIGN as the state's official electronic signature and record legislation.

2. Preemption and Technological Neutrality

Section 7002(a)(2)(A)(ii) states:

[Any state statute, regulation, or other rule of law may modify, limit, or supersede the Act only if] (ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.

E-SIGN, therefore, also requires any state considering whether to supersede the Act with its own home-grown legislation to make the state


In such cases—and nearly all of the states that have adopted UETA to date fall into this category—a key question of interpretation will be whether the consistency standard should be applied to the entirety of the non-conforming version of UETA or, rather, applied only to the non-conforming provisions. See Wittie & Winn, supra note 199, at 329.

"Presumably non-substantive changes, such as formatting, section numbering and the like, would not be enough to cause a state's version of UETA not to be considered the 'official' version for purposes of E-SIGN section 102(a)(1)." Id. at 329 n.185.


325. 15 U.S.C.A. § 7002(a)(2)(A)(i). If a state adopts the official UETA and a UETA provision is not consistent with E-SIGN, a state may adopt the corresponding E-SIGN provision as part of a valid and consistent non-conforming version of UETA. See also Wittie & Winn, supra note 199, at 329 (discussing the adoption of the E-SIGN consent provision as part of a non-conforming version of UETA).

legislation technologically neutral.327 Nevertheless, the authority of states to "modify, limit, or supersede" E-SIGN creates the potential for nonuniformity because the definition and application of "technical neutrality" has yet to be examined and interpreted by either the courts or the leaders in the electronic commerce field.328

Questions remain . . . as to how far this provision does go, particularly with respect to the use of authentication technologies—sometimes referred to as security procedures—designed to verify the identity of the sender of an electronic record or to ensure that the content of an electronic record has not been altered. The legislative history reflects this provision was 'intended to prevent a state from giving a leg up or impos[ing] an additional burden on one technology or technical specification that is not applicable to all others.'329

The federal government has stressed the necessity of "technological neutrality" in e-commerce legislation:330

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

327. Id.
328. See Wittie & Winn, supra note 199, at 334 n.202. "One commentator has suggested that, since E-SIGN section 101 does not address giving preferential treatment to particular technologies, a law that merely "gives enhanced effect to any particular technology" is unaffected by the technology neutral standard." See also Raymond T. Nimmer, Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws (discussion draft, Aug. 11, 2000), available at http://www.bmck.com/ecommerce/whatsnewesignatures.htm. Based on this, Professor Nimmer argues that a statute providing that "signatures that use XYZ technology and certification procedures establish a presumption that they are the records or signatures of the person identified by the technology" would not be preempted because E-SIGN section 101 does not deal with attribution issues. Id. This argument goes too far, however, effectively reading the words "accord greater legal status or effect to" out of the Act.
329. See Wittie & Winn, supra note 199, at 334. "The same statement in the legislative history, however, is careful to point out that the provision is not intended 'to prevent a state . . . from developing, establishing, using or certifying a certificate authority system.' " See 146 CONG. REC. S5285 (daily ed. June 16, 2000) (statement of Sen. Spencer Abraham).
330. See Smedinghoff & Bro, supra note 32, at 760. In fact, technical neutrality 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., the rules should neither require nor assume a particular technology.)' 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.

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.\textsuperscript{331}

E-SIGN's "technological neutrality" standard appears to focus its attention on state legislation that mandates or prefers a particular technology for electronic record and signature authentication, and those that do not.\textsuperscript{332} Consequently, so-called "digital signature" laws\textsuperscript{333} that afford validity and enforceability only to the use of one
termed the 'message' in these Guidelines. Then a hash function in the signer's software computes a hash result unique (for all practical purposes) to the message. The signer's software then transforms the hash result into a digital signature using the signer's private key. The resulting digital signature is thus unique to both the message and the private key used to create it.

Typically, a digital signature (a digitally signed hash result of the message) is attached to its message and stored or transmitted with its message. However, it may also be sent or stored as a separate data element, so long as it maintains a reliable association with its message. Since a digital signature is unique to its message, it is useless if wholly disassociated from its message.

Verification of a digital signature is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks: (1) whether the digital signature was created using the corresponding private key; and (2) whether the newly computed hash result matches the original hash result which was transformed into the digital signature during the signing process. The verification software will confirm the digital signature as 'verified' if: (1) the signer's private key was used to digitally sign the message, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will verify only a digital signature created with the signer's private key; and (2) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

Various asymmetric cryptosystems create and verify digital signatures using different algorithms and procedures, but share this overall operational pattern. To verify a digital signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key. However, a public and private key pair has no intrinsic association with any person; it is simply a pair of numbers. Some convincing strategy is necessary to reliably associate a particular person or entity to the key pair.

In a transaction involving only two parties, each party can simply communicate (by a relatively secure 'out-of-band' channel such as a courier or a secure voice telephone) the public key of the key pair each party will use. Such an identification strategy is no small task, especially when the parties are geographically distant from each other, normally conduct communication over a convenient but insecure channel such as the Internet, are not natural persons but rather corporations or similar artificial entities, and act through agents whose authority must be ascertained. As electronic commerce increasingly moves from a bilateral setting to the many-on-many architecture of the World Wide Web on the Internet, where significant transactions will occur among strangers who have no prior contractual relationship and will never deal with each other again, the problem of authentication/nonrepudiation becomes not merely one of efficiency, but also of reliability. An open system of communication such as the Internet needs a system of identity authentication to handle this scenario.

To that end, a prospective signer might issue a public statement, such as: 'Signatures verifiable by the following public key are mine.' However, others doing business with the signer may for good reason be unwilling to accept the statement, especially where there is no prior contract establishing the legal effect of that published statement with certainty. A party relying upon such an unsupported published statement in an open system would run a great risk of trusting a phantom or an impostor, or of attempting to disprove a false denial of a digital signature ('nonrepudiation') if a transaction should turn out to prove disadvantageous for the purported signer.

The solution to these problems is the use of one or more trusted third parties to associate an identified signer with the specific public key. That trusted third party is
particular authentication technology would not satisfy the technical neutrality standard of E-SIGN and, therefore, would be preempted.\textsuperscript{334} Utah's digital signature legislation is a statute that would be subject to this preemption analysis.\textsuperscript{335} Legislation that does not mandate or promote a particular technology, but rather is less "technologically specific," may resist the preemption power of E-SIGN.\textsuperscript{336} Therefore, a "Clintonesque" use of semantics will not serve state legislatures well

\begin{itemize}
\item referred to as a 'certification authority' in the most technical sense and in these Guidelines.
\item To assure both the message and identity authenticity of the certificate, the certification authority digitally signs it . . . .
\end{itemize}


\textsuperscript{334} See Wittie & Winn, \textit{supra} note 199, at 334.

\textsuperscript{335} The Utah Digital Signature Act assigns legal significance only to the use of one particular electronic signature technology—"asymmetric crytosystems." \textbf{Utah Code Ann.} § 46-3-101 to 46-3-501 (1998). Section 46-3-103(10) of the Utah Code Annotated defines "digital signature" as:

\begin{itemize}
\item a 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:
\item (a) the transformation was created using the private key that corresponds to the signer's public key; and
\item (b) the message has been altered since the transformation was made.
\end{itemize}


Utah Code section 46-3-103 (2) provides: "Asymmetric cryptosystem means an algorithm or series of algorithms which provide a secure key pair." \textbf{Utah Code Ann.} § 46-3-103 (2) (1998).

Utah Code section 46-3-401 provides:

\begin{itemize}
\item (1) Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature if: (a) that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority; (b) that digital signature was affixed by the signer with the intention of signing the message; and (c) the recipient has no knowledge or notice that the signer either: (i) breached a duty as a subscriber; or (ii) does not rightfully hold the private key used to affix the digital signature.
\end{itemize}


\textsuperscript{336} The Illinois Electronic Commerce Security Act provides on the one hand that electronic signatures and records cannot be denied legal effect merely because they are in electronic form, and on the other hand, that highly secure forms of electronic signature will be given preferred legal status. See Wittie & Winn, \textit{supra} note 199, at 335. See \textbf{5 Ill. Comp. Stat. Ann.} 175/1-105 to 175/99-1 (West 1993 & Supp. 2000). Section 5-105 provides: "‘Electronic signature’ means a signature in electronic form attached to or logically associated with an electronic record." \textit{Id.} § 5-105. Section 10-105 (a) provides:

\begin{itemize}
\item If, through the use of a qualified security procedure, it can be verified that an electronic record has not been altered since a specified point in time, then such electronic record shall be considered to be a secure electronic record from such specified point in time to the time of verification, if the relying party establishes that the qualified security procedure was: (1) commercially reasonable under the circumstances; (2) applied by the relying party in a trustworthy manner; and (3) reasonably and in good faith relied upon by the relying party.
\end{itemize}

\textit{Id.} at § 10-105 (a).
during the development and drafting of electronic signature legislation; “if a law is phrased in terms of performance standards that in reality can only be met by a particular technology, it seems likely that it will not be considered technically neutral for purposes of the Act.”

C. Repeal the Statute of Frauds

E-SIGN explicitly renounces any distinction between paper-based and electronic transactions, thereby “amending” the Statute of Frauds to comport with this technological era as did the examples of state reforming legislation. Consequently, the Statute of Frauds’ “continued vitality has come into question as its rationales have eroded and as computer technology makes outdated the 'signature' and 'writing' requirements.”

Some commentators have suggested repealing the Statute of Frauds. These scholars have suggested this course of action in light of the continued vitality of the Statute of Frauds as its foundations have eroded, and the growth of Internet technology has illustrated the outdated nature of the “signature” and “writing” requirements. Proponents of a repeal assail the Statute on three grounds. First, they argue that the Statute of Frauds is “inconsistent with current business customs.” Second, proponents contend that the Statue of Frauds should be repealed because it has too many exceptions and exclusions. Under the U.C.C., “better than 80 percent of the statute of frauds cases that are reported are cases that come within one of the exceptions to the writing requirement.” Finally, proponents of repeal assert that the Statute of Frauds “tends to produce litigation, and thus, taxes judicial resources.” These critics ironically argue that a repeal of the Statute of Frauds will decrease fraud by prohibiting parties from avoiding otherwise enforceable contractual duties.

The states, however, have chosen to amend the Statute of Frauds instead of repealing a critical foundation of contract law. In main-

337. See Wittie & Winn, supra note 199, at 336.
339. See Overby, supra note 18, at 225.
341. Id.
342. Id.
343. Id. at 441.
344. Id. at 439.
345. Id. at 441.
346. See Szafran, supra note 6, at 519.
347. Id. at 509-511.
taining the very foundation of its existence, the Statute of Frauds "can prevent – and for various circumstances arising outside the scope of electronic-based contracts has prevented – the occurrence of fraudulent transactions and unfounded claims."\textsuperscript{348} One commentator noted:

Initiating an all-encompassing repeal of the Statute would effectively dismiss the benefits section 2-201 arguably provides for particular transactions. As much of an obstacle as the Statute poses for some transactions (including but not limited to electronic), when section 2-201 prevents fraudulent practices and unfounded claims, its value becomes indisputable. Furthermore, common law experience indicates that in many circumstances the Statute of Frauds has provided reliable evidence that a contract was formed. In this capacity, it serves as a potent antidote to fraud and perjury.

[An additional] argument against complete recission stems from the commercial community's traditionally strong resistance to repeal; the instinct to oppose suggestions that could eliminate objective evidence of what constitutes a contract remains deeply rooted. The reason for the legal and business communities' aversion is not difficult to understand: fraudulent practices are likely to occur in the business environment. Thus, any proposal to eradicate a doctrine whose purpose is to prevent fraud will almost certainly be met with resistance. This response is founded in the security and assurance the business community finds in the Statute's formality and tradition. After all, when commercial disputes must be resolved, written evidence presented to the trier of fact can at least provide threshold protection to the litigant.

Finally, the Statute's core value is evident in its capacity to protect against enforcing questionable or nonexistent oral agreements and preventing a party from evading an obligation deliberately incurred. Thus, section 2-201's role as a deterrent to fraud may, in and of itself, justify its retention . . . . Discarding the Statute altogether given the worthwhile benefits it periodically provides is draconian and can only result in a "reform" as inefficient as the original problem.\textsuperscript{349}

V. IMPACT

While E-SIGN has sown the seeds of confidence in the business and commercial sectors, the Act is silent as to which technologies and other authentication procedures are to be used to manifest this confidence into palpable paperless transactions. Furthermore, electronic contract integrity is a crucial obstacle that must be tackled by the private sector. The private sector and the marketplace are resigned to develop the most efficacious infrastructure to deal with these technical complexities, thereby reducing the increased risk of liability associated

\textsuperscript{348} Id.
\textsuperscript{349} Id.
with the use of contemporary technology to further develop the arena of commercial transactions.

A. The Systems and Procedures Needed for Secure Electronic Transactions

Although E-SIGN was designed to force states to adopt uniform legislation in electronic contracting, it leaves many gaps to be filled.\textsuperscript{350} Although the enforceability of electronic contracts is validated and businesses may be encouraged to rid themselves of paper, businesses must develop systems and procedures that prove that the records have not been tampered with, that the signatures are accurate, and that all parties to the transaction know who has consented to the agreement.\textsuperscript{351}

\begin{footnotesize}
\footnote{350. See Zoelick, supra note 2, at 10. Authentication involves determining the identity of the parties to a transaction so that the parties are certain that they are dealing with whom they purport to deal:

Today, a large percentage of electronic commerce retail transactions are between parties that do not have a pre-existing business relationship and do not meet face-to-face. Thus, traditional methods of identifying a party and conducting a legally binding transaction can be completely absent. Once the identity of the parties has been established, it is important that the online transaction take place in a secure environment to ensure the authenticity and integrity of the transmission and that a record of the transmission is retained should any dispute arise in the future. Technology, such as electronic signatures, providing a solution and resolving many of the complex issues involved in online commercial transactions.}

\footnote{351. The main objection to the electronic transmission of contracts is that the content of the contract can be altered and forged:

Yet, the same fate can befall information stored on paper documents. While the statute of frauds offers some level of protection, it does not protect against all fraud and perjury. New technological developments initially can make the detection of forgeries difficult. Techniques soon will emerge, however, that provide parties and courts with a reliable method of determining the authenticity of the data. Furthermore, the threat of persistent computer hackers bypassing security features does not mean that the guarded computer messages lack evidentiary value: if one in a billion computer messages is counterfeit, then a computer message is more likely authentic than not.

Intentional alteration of messages is not the only concern relating to electronic messaging. Messages that must be translated from one format to another, either by a third party network during transmission or upon receipt, could be unintentionally altered during the translation. To prove the authenticity of a ‘signed’ computer message, a party must show that the ‘signature’ relates to the content of the message and that the message has not been altered since it was originally signed.

Few guidelines exist to control paper documents and even fewer to control electronic documents. In the paper world, contracting parties write with nonerasable ink, sequentially number document sheets, bind or staple pages, and require signatories to initial individual pages or paragraphs. While mistakes are just as likely to occur under paper-trading conditions, the speed of computer communication causes mistakes to happen rapidly, successively, and free of visible controls.}
\end{footnotesize}
E-SIGN intentionally avoids specifying or mandating the technological procedures that are required to validate an electronic contract.\textsuperscript{352} This intention may be based on the knowledge and anticipation of vast growth in the technology industry. This stance, however, leaves many issues to be resolved with respect to the proper presentation and authentication of electronic contracts.

Without a technological mandate, the true problems with electronic contracts become visible. These problems are "message integrity" and "sender authenticity."\textsuperscript{353} The use of encryption\textsuperscript{354} would likely resolve any difficulties with respect to ensuring the integrity of the electronic message in an electronic transaction. Encryption, coupled with the use of electronic signatures, is currently capable of ensuring the integrity of an electronic message.\textsuperscript{355} One may be certain, as a result,

Computer companies have developed, and continue to improve, a multitude of security measures and check systems. New systems continually emerge and old systems improve. Software companies can provide their customers with editing programs that flag mistakes in transmission, whereby parties on either end of the transmission can fix the mistakes to ensure a relatively error-free contract. Parties can agree on secret codes and passwords to insure proper authorization and authentication. Receiving parties can send a return acknowledgement reciting the material provisions of the contract. These check systems and others allow parties to detect and quickly remedy human or computer errors.

Adequate security procedures are critical to effective electronic communication. Each party must bear the risk and responsibility of using adequate restrictions on access to its 'signature' and adequate security in the storage of computer records. The law should make it to each party's advantage to use those security procedures that both reasonably ensure all transmissions of documents are authorized and protect business records from improper access.

See Wilkerson, supra note 49, at 419.

\textsuperscript{352} 15 U.S.C.A. § 7002(a)(2)(ii). E-SIGN simply does not say what an electronic signature is, or what technology may or should be used to procure a sufficient mechanism to comply with the Act, and the UETA. See Zoelick supra note 2, at 11-18.

Before companies will accept electronic signatures they need to know when to trust them as authentic and when not to. Just as [E-SIGN] leaves it to the market to sort out useful electronic signature technologies from those that are not secure, convenient, or are flawed in some other way, [E-SIGN] also leaves it to the market to develop useful mechanisms for validating signatures and establishing trust in electronic documents.

\textit{Id.}

\textsuperscript{353} To understand message integrity and sender authenticity, one must understand how digital signatures work. See Marc J. Lane, Check Out the Fine Print Before Using Electronic Signatures, CRAIN'S CHICAGO BUSINESS, January 8, 2001, at 13. See also Zoelick, supra note 2, at 14.

\textsuperscript{354} Encrypting messages keeps them private, and encryption may be used to maintain message authenticity and integrity. Pioneered by the federal government for use in wartimes, encryption technology is demonstrating its usefulness in the arena of complex commercial transactions. Public Key, coupled with Private Key, encryption allows a computer to oversee an electronic transaction whereby other parties are prevented from interfering with the transmission, specifically, the integrity and authenticity of the paperless transaction.

\textsuperscript{355} See Zoelick, supra note 2, at 14.
that the message received in the formation of an electronic contract was in fact the message that was sent.

But what if businesses do not encrypt their electronic messages? The current reality is that an extraordinary number of businesses do not encrypt their e-mail, creating a substantial barrier to the integrity of electronic messages ultimately used for the formation of electronic contracts. E-SIGN does not address the issue of message integrity, but it does leave the decisions regarding the trustworthiness of electronic communications in the hands of the market. Although E-SIGN induces the business sector to leave paper-based transactions behind, the absence of message integrity in E-SIGN mandates a significant analysis by those businesses. This inquiry must include an analysis of the costs, benefits, and risks associated with developing and implementing a system to establish the integrity of the electronic messages that will form the foundation for significant commercial transactions.

But message integrity may be the least complex formality facing businesses as they contemplate electronic commercial transactions. Authentication of the electronic messages is the Goliath of difficulties businesses will face. Why should you trust that a party's electronic signature subscribed to an electronic contract is in fact her signature and her intent to authenticate the communication? Even if an electronic communication sufficiently meets the requirements of a writing and it contains an electronic mechanism that renders the communication signed, which brings it within the ambit of legal validity and enforceability pursuant to E-SIGN and the Statute of Frauds, the party seeking to enforce the electronic contract must prove that the promise contained in the electronic message was in fact made by the party against whom enforcement is sought.

E-SIGN, with its focus on technical neutrality, does not supply a mandate or even a roadmap with respect to authentication technologies. Many browsers now contain authentication features, and busi-
nesses are developing pen-based and other technologies to facilitate the authentication of electronic contracting. Before businesses dive head-first into exposing their companies and shareholders to the substantial risks of electronic contracting by placing their electronic signatures upon an electronic communication, the technology sector must establish the mechanisms for authenticating the electronic signatures and the concomitant electronic message. Just as E-SIGN gives to the market the responsibility of formulating useful electronic signature technologies, it also forces the market to develop efficient mechanisms for authenticating electronic signatures and establishing the veracity of the electronic communications to which they are ascribed.

B. The Liability Exposure of Electronic Transactions

E-SIGN is evidence of a tremendous breakthrough in the area of contract law. The Act, through its amendment of the Statute of Frauds, creates uniformity across both state and international boundaries. This process, however, takes time.

The evolution of contract law to encompass electronic transactions will expose parties to electronic contracts to increased liability in the immediate term. From jurisdictional issues to evidentiary presumptions, E-SIGN will increase the attention paid to electronic transactions traditionally executed under the auspices of state law.


360. See Zoelick, supra note 2, at 14.

361. Id. at 18.

362. See supra notes 263–293 and accompanying text.

363. See Lane, supra note 353, at 13:

There remains the real possibility that an unauthorized person can gain access to one’s private keys and ‘sign’ documents in one’s name. And a phony public key can cause the verification software to give the thumbs-up to a bogus message. That’s why, one day soon, biometric authentication—whether by fingerprint, voice, DNA or iris—likely will replace public key infrastructure and change the way business is done. For now, the online public may be wary of an online contracts system. And the opportunities E-SIGN presents, while a healthy signal of the government’s enthusiastic support of electronic commerce, should be considered with caution. Id. at 13.

364. See Robertson, supra note 54, at 827. “The drafters of uniform legislation and state statutes relating to electronic commerce have confronted these issues. Unfortunately, the issue of ‘binding’ an individual to an electronic message has led to many different and inconsistent approaches.” Id. In digital signature legislation, specifically the Utah statute: [T]he court shall presume that the digital signature is that of the person listed in the certificate, that it was affixed by that person with the intention of signing the message,
Electronic signatures and records require new and evolving technology that has yet to be analyzed by the courts. The use of electronic contracting in the world of commercial transactions will inevitably raise questions about party responsibility in the case of a breach, or more worrisome, in case of a failure of technology. Consider the following hypothetical:

Cedric, a licensed certification authority, duly issues a certificate to Susan, who accepts it. Cedric publishes the certificate in a recognized repository. Susan's private key, which corresponds to the public key in the certificate, is kept on floppy disk. Irving, a malicious computer hacker, releases a computer virus on the Internet that finds its way onto Susan's computer. Subsequently when Susan uses her private key, the virus program surreptitiously sends a copy of Susan's private key to Irving. Irving immediately uses the private key to cash a $10,000 electronic check drawn upon Susan's account payable to a numbered, anonymous account in a state having rigorous bank secrecy laws. Irving disappears and cannot be found. As soon as Susan learns of the fraud she revokes her certificate.

Who covers the $10,000 loss? Susan's first hurdle if she wants to avoid the $10,000 loss is to repudiate the false signature. The Electronic Signatures Act does not say what the standard for non-repudiation should be.

E-SIGN does not address the liability issues associated with authentication technologies, certification authorities, or the falsification of electronic signatures or electronic messages. These liability concerns are left to the states or the Uniform Commercial Code. These issues, however, are not effectively managed by existing laws and regulations concerning paper-based transactions. Given the lack of at-

and that the recipient had no notice that the signer breached any duty owed to the CA or does not rightfully hold the private key used to create the signature.

Id. at 832.

365. See Zoelick, supra note 2, at 15. See also Uniform Commercial Code Article 9. The definition of chattel paper pursuant to § 9-102 includes electronic documents:

Under former section 9-105, only if the evidence of an obligation consisted of 'a writing or writings' could an obligation qualify as chattel paper. In this Article, traditional, written chattel paper is included in the definition of 'tangible chattel paper.' 'Electronic chattel paper' is chattel paper that is stored in an electronic medium instead of in tangible form. The concept of an electronic medium should be construed liberally to include electrical, digital, magnetic, optical, electromagnetic, or any other current or similar emerging technologies.

Id. at cmt 5.

366. See Zoelick, supra note 2, at 15.


368. See Zoelick, supra note 2, at 15.

369. Id. at 12.

370. Id.

371. Id. at 18.
tention paid to these issues by E-SIGN, an era of potentially large liabilities associated with the use of electronic signatures and records faces business until there is more experience, legal precedent, and possibly legislation dealing with electronic contracting.372

VI. CONCLUSION

It has been a long and arduous journey from the origins of the Statute of Frauds to the Electronic Signatures in Global and National Commerce Act, which was driven by the ever-expanding world of Internet technology. Electronic transactions have facilitated fundamental changes in the bedrock of contract law. Will its foundations become too weak?

The core changes to contract law are driven not by a disgust of the present system, but rather by a look towards the future. The legal profession has entered a time whereby we must assure the business and technology communities that the traditional framework of paper-based regulation of commercial transactions will not hinder the growth of the modern business environment. Congress has given that assurance by enacting E-SIGN.

The legal change effected by E-SIGN is simple: parties seeking to engage in business through electronic means may mutually consent to use electronic signatures and electronic records. These electronic contracts will have the same legal validity and enforceability as their paper-based counterparts. This simple alteration in the law, however, has the potential to create a substantial reformation in business and consumer behavior.

Although, the clear intent of E-SIGN is to establish the legal validity and enforceability of electronic contracting, E-SIGN will not assume the role of a dynamic catalyst for a new revolution in electronic commerce. Despite the clear indication of the government's enthusiastic support of electronic commerce, the market is still faced with crucial decisions about the use and trustworthiness of electronic signatures and electronic records.

Steven Domanowski

372. Id.