UIC John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 2 *Journal of Computer & Information Law - Winter 2001*

Article 5

Winter 2001

Fair Warning: Preemption and Navigating the Bermuda Triangle of E-Sign, UETA, and State Digital Signature Laws, 19 J. Marshall J. Computer & Info. L. 401 (2001)

Renard Francois

COMMENT

FAIR WARNING: PREEMPTION AND NAVIGATING THE BERMUDA TRIANGLE OF E-SIGN, UETA, AND STATE DIGITAL SIGNATURE LAWS

I. INTRODUCTION

While Internet transactions are a small percentage of total business transactions, the amount of business being conducted over the Internet is growing.[1] For the Internet to continue to grow, consumers and businesses must be confident that electronic transactions are safe and reliable.[2] One impediment to the prolonged growth and increased consumer comfort in using e-commerce is the fear of fraud,[3] which can occur in two ways.[4] First, the inability to authenticate, which is the method of determining the identity of the other party, can lead to fraud.[5] Transactions

1. David L. Gripman, *Electronic Document Certification: A Primer On the Technology Behind Digital Signatures*, 17 John Marshall J. Computer & Info. L. 769, 770 (1999).

2. *Id.*

3. *See Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth*, Congressional Research Serv. Rpt., 107th Cong. 11 (Jan. 31, 2001) [hereinafter *Internet*]. The Department of Commerce reported that approximately four million people were using the Internet, and in one year the number of Internet purchasers rose to ten million. *Id.* It has been estimated that the amount of retail transactions generated domestically would top seven billion dollars by the end of 2000. *Id.* Additionally, despite the slow down of the economy and the large numbers of dot.com companies going out of business, e-commerce continues to grow, though not at the robust rate of growth of the past year. *Id.* Worldwide, e-commerce will continue to grow at a rapid rate because North America has the most Internet users with 56.5 percent. *Id.* And while the Asian Pacific region has nearly 16 percent of the world's Internet users, the rate of new users is growing at a rate that is twice as fast as North America. *Id.*

4. Dan McGuig, *Halve the Baby: An Obvious Use to the Troubling Use of Trademarks as Meta Tags*, 18 John Marshall J. Computer & Info. L. 643, 645-46 (2000). Meta tags are a form of Hyper Text Markup Language that surreptitiously provides information that is not displayed to the person viewing that page. *Id.* at 646. The form of meta tag relevant for this comment is the key word, which allows a search engines to find Web sites of a particular description. *Id.*

5. Thomas Smedinghoff, *Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing Commerce*, John Marshall J. Computer & Info. L. 735, 745 (1999).

of dubious authenticity potentially expose a business to pranks that waste valuable time and resources.[6] For example, if Amazon.com sends a book to a person Amazon thinks ordered the book but in reality the person neither wanted nor ordered anything from Amazon, Amazon loses the price of obtaining and shipping the product.

Second, difficulty in verifying the integrity of a transmission can lead to fraud.[7] Before the parties can feel comfortable negotiating and transacting business electronically, they must be comfortable in knowing that the content of the transmissions are accurate and complete.[8] A contractor who gathers bids from subcontractors electronically must be certain that the bids submitted by the subcontractors are accurate and complete.[9] When there is difficulty establishing either the authenticity of the sender or the integrity of the transmission, it is easier for parties to repudiate their contracts.[10] Concerns about authenticity, integrity, and repudiation can create a significant barrier to using the Internet for transactions and negotiations.[11] To avoid these potential problems, a business must do a significant amount of their transactions outside of the e-commerce framework.[12]

For example, just because a message has the name Alden Hitchcock Smith III at the bottom of a document, it does not mean that Alden Hitchcock Smith III has actually signed the document or that someone else was authorized to sign his name.

6. *Id.*

7. *Id.* at 746. Integrity of a document relates to whether the document received by the sender is the same as the one sent. *Id.* Alden Smith may send a message to his attorney requesting certain confidential information. While Alden's attorney is certain that Alden sent the message, the attorney may be just as uncertain about whether or not the communication has been intercepted or altered by an unauthorized third party, or that the message transmitted was the complete message. While this example shows that there are issues arising out of the actions of unscrupulous and deceitful parties, issues relating to the integrity of a message can occur in innocuous instances, such as a message being garbled or an interrupted during transmission. *Id.*

8. *Id.*

9. *Id.* (citing *Victory Med. Hosp. v. Rice*, 493 N.E.2d 117 (Ill. App. 1986)). The example in the text deals with a mistake or an alteration to the content during transmission. A more nefarious example is when a party actively engages in fraud. For example, computers can produce documents that are virtually indistinguishable from the original document. One party can easily alter material provisions of the original document and claim that the altered document is the original. Should two parties dispute the integrity of the other's document, it would be very difficult, if not impossible, to determine which party had the original document and to enforce those provisions of the contract.

10. Smedinghoff, *supra* n. 5, at 746.

11. While this paper uses the term "consumer" quite often, the term as used in this paper envisions the consumer being another business. It is important to remember that the fastest growing sector of e-commerce is business-to-business exchanges. *Internet*, supra n. 3, at 12. Domestic business-to-business transactions topped $200 billion in 2000 and will exceed $1.2 trillion by 2003. *Id.*

12. The Internet gives businesses the opportunity to significantly reduce their advertising costs by allowing small and medium sized businesses to electronically control their

To work within the e-commerce framework,[13] businesses turn to encryption.[14] Electronic signatures and digital signatures are the present day method of hiding the information in a transmission.[15] Digital signatures promote the increased growth and development of e-commerce.[16]

---

supply chain management, after sales support, and payment. *Id.*; *see* Mary Jo Dively, *The New Laws that Will Enable Electronic Contracting: A Survey of Electronic Contracting Rules in the Uniform Electronic Transaction Act and the Uniform Computer Information Transaction Act*, 38 Duq. L. Rev. 209, 212 (2000) (stating that time, efficiency, and storage space are benefits of electronic commerce); *but see* Bob Tedeschi, *Large Companies Try to Find Ways to Spread Internet Retailing Throughout Their Operation*, N.Y. Times C14 (Oct. 15, 2000) (discussing large businesses working to create a sound business strategy for entering e-commerce); Bob Tedeschi, *Compressed Data: Big Companies Go Slowly in Devising Net Strategy*, N.Y. Times C4 ¶ 3 (Mar. 27, 2000) (discussing why business are so slow in entering the area of e-commerce).

13. David Streitfeld, *E-Commerce The Play: Act II: Bricks and Clicks Get Together*, Washington Post H01 ¶ 34 (Oct. 22, 2000). E-businesses can not only create Web sites containing product information but also use strategic alliances with other businesses to attract consumer interest and customers at a cost that is significantly cheaper than traditional means of advertising. *See id.* at ¶ 34. Sneech.com—a DVD, game, and audio book retailer—epitomizes the low cost e-business company by having two employees, no office space, virtually no advertising, no interest on loans, and an invested capital of approximately $2,000. *Id.* Sneech.com, before creating and launching its Web site, entered into a strategic alliance with Yahoo! in which for $100 a month, Yahoo! would place Sneech.com on a shopping list with approximately 12,000 other merchants. *Id.* After offering a limited number of products, Yahoo! offered Sneech.com the opportunity to become a featured shopping partner, and Sneech.com went on to create their own Web site and increased sales. *Id.* The explosion of e-commerce has personal benefit as well. Rep. George W. Gekas, *Early Returns from Government Regulation of Electronic Commerce: What's New Is What's Old*, 51 Admin. L. Rev. 769, 771 (1999). E-commerce reduces the cost of goods and services on the one hand, and frees up people's time on the other; everyone may expect to have more money to spend and more time to devote to living better lives. *Id.* E-commerce literally means that, directly or indirectly, everyone gets more, including more food, better health care, stronger families, and a better environment. *Id.* E-commerce has even benefited small communities. *See* Larry Tye, *In Haverhill, An Identity Crises Battered City Struggles to Find a Sense of Community*, Boston Globe A1 ¶ 20 (Feb. 20, 2001) (mentioning that cyber district and e-commerce played a significant role in the boom of a local economy).

14. Gripman, *supra* n. 1, at 774. Cryptography is the art of keeping information secure and disguising a message in such a way that the substance of the message is not readily understandable. *Id.* Disguising messages to keep them secure has been in practice since antiquity, as when Lysander of Sparta used encryption to communicate with his soldiers on the battlefield. *Id.*

15. W. Everett Lupton, Student Author, *The Digital Signature: Your Identity by the Numbers*, 6 Rich. J.L. & Tech. 10, ¶ 5 <http://www.richmond.edu/jolt/v6i2/note2.html> (Fall 1999). In fact, electronic signatures are a combination of signature and code, which is the method of changing a letter or a group of letters into another group of letters or symbols. *Id.* In the computer context, the encryption software applies a mathematical algorithm to the plain text, the readable text, which then produces unreadable cipher text. Gripman, *supra* n. 1, at 774.

16. Sanu K. Thomas, Student Author, *The Protection and Promotion of E-Commerce: Should There Be a Global Regulatory Scheme for Digital Signatures*, 22 Fordham Intl. L.J. 1002, 1008 (1999).

By addressing concerns of authenticity and integrity, electronic and digital signatures give businesses a measure of comfort in negotiating and transacting electronically.[17]

Section one of this comment examines the digital signature legislation throughout the U.S. to determine if such legislation does, in fact, remove these barriers to e-commerce and provide a clear and easy framework for conducting business electronically. Section two provides general background information regarding digital and electronic signatures. Specifically, the section briefly describes the types of state laws that were enacted to govern the use of digital and electronic signatures. After introducing the federal legislation, section three discusses the preemption provisions of the new federal law. Specifically, section three assesses the impact of the preemption clause on the tapestry of existing state digital signature laws and the Uniform Electronic Transactions Act ("UETA"). This comment concludes by suggesting a new preemption provision that does not place onerous requirements on the parties desiring to conduct business electronically and provides clarity and precision that is lacking in current federal, state, and uniform signature laws.

II. BACKGROUND

Over forty states have enacted digital and electronic signature legislation.[18] The Utah Digital Signatures Act (the "Utah Act") was the na-

17. *See* Thomas J. Smedinghoff, Presentation, *Digital Signatures: The Key to Secure Internet Commerce* at 8 (Glasser Legal Works 1998); *but see* Jane K. Winn, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, Revised Draft Mar. 9, 2001 <http://www.smu.edu/~jwinn?shocking-truth.htm> (accessed Apr. 16, 2001) (discussing theories as to why the use of digital signatures "have not lived up to the hype"). There can be a great deal of confusion when reading literature about digital and electronic signatures. Smedinghoff, *supra* n. 5, at 728 (endnote omitted). Much of the confusion results from the sloppy use of the terms digital signature and electronic signature. An electronic signature can be almost anything because it is commonly defined to be "any electronic mark signifying agreement" to a transaction. Lupton, *supra* n. 15, at ¶ 5. More recent definitions of electronics signatures broaden the term so much that sounds or a retinal scan of the party would be considered an electronic signature. *Id.* In any event, regardless of the statute defining the term, most definitions have four characteristics that are indicative of an electronic signature: (i) the sound, mark, or symbol must be in electronic form; (ii) there must be an intent by the signor to transmit that sound, mark, or symbol; (iii) an intent to be bound by the terms and (iv) there is no specific technology described. On the other hand, a digital signature is not, as some would think, a digitized version of one's signature but rather pieces of electronic communication transmitted between the sender and the recipient. *Id.* at ¶ 7. Technically, a digital signature is the "transformation of a message using an asymmetric crypto-system or a hash function such that a person having the initial message and the signer's public key can accurately determine if the holder of the private key sent the message and if the message has been altered in some way. *Id.* at ¶ 10.

18. Thomas, *supra* n. 16, at 1010. Before the attempts to create a uniform law relating to signatures and e-commerce, state legislation could be classified into three categories.

tion's first comprehensive digital and electronic signature legislation.[19] The Utah Act, interestingly, was not broad enough to give legal protection to both digital signatures and electronic signatures.[20] Under the Utah Act, as well as under the statutes of other states following the mode of the Utah Act,[21] digital signatures receive legal protection only if

Smedinghoff, *supra* n. 5, at 739-42. Statutes that only give legal effect to digital signatures that are the product of a specific technology—technology specific statutes. *Id.* The second type of statutes are those that do not require a digital signature to be the product of a particular technology but do establish certain criteria that the method of affixing a digital signature must satisfy to receive legal effect. *Id.* at 738. These statutes are attribution statutes. Finally, enabling statutes neither prescribe a specific technology nor establish certain criteria that the signature method must satisfy. *Id.* at 742. Essentially enabling statutes parallel the common law statute of frauds paper-writing requirement, which gives legal effect to a signature as long as (i) there is a writing; (ii) a signature on the writing; and (iii) the signature must be by the person or an agent of the person to be bound by the contract's terms. *E.g.* S.C. Code Ann. § 26-5-30 (2000) (defining electronic signature "any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the party using it to have the same force and effect as a manual signature.").

19. Utah Code Ann. §§ 46-3-101 *et seq.* (1999). Utah created the law so that, inter alia, relying on secure messages would increase the number of e-commerce transactions and minimize the amount of forgeries and fraud occurring in e-commerce. *Id.* at § 46-3-102. A valid digital signature is one that has the same effect as a traditional signature if the document bears "in its entirety the digital signature," and the digital signature is verified by a public key listed on a certificate issued by a licensed certification authority. *Id.* §46-3-401(a)-(b).

20. *Id.* §46-3-103(10). There are two types of digital signature encryption: symmetric key cryptography and asymmetric key cryptography. Gripman, *supra* n. 1, at 773-75. Symmetric key cryptography is a method in which the sender and recipient of a message use the same key to encrypt and to decrypt the message. *Id.* at 773. In the digital world, the sender of a message uses an algorithmic key to translate information from plain text to cipher-text. *Id.* at 774. In order to decrypt the message, the recipient must use the same key that the sender used to encrypt the message. *Id.* Symmetric key cryptography is not altogether unfamiliar in the U.S. In 1977, the U.S. adopted a Data Encryption Standard, which was based on a symmetric algorithm. *Id.* at 775. One of the most significant problems with symmetric cryptography is maintaining the secrecy of the key. Thomas, *supra* n. 16, at 1009.

21. Gripman, *supra* n. 1, at 775. In the digital era, the use of symmetric key encryption is rife with security complications that would severely compromise the benefit of transacting business over the Internet. *Id.* First and foremost, because sender and recipient use the same key, it is imperative that both parties protect the secret key. *See* Thomas, *supra* n. 16, at 1010. In the event a third party discovers the secret key the third party, at the very least, could read the encrypted message. *Id.* At worst, by having the secret key, the third party may intercept, read, alter, or send messages without the recipient having any reason, on the face of the transmission, to assume that the sender is an unauthorized third party. *Id.* Another security problem arises when the parties have to transmit information about the secret key over the Internet which is not secure. *Id.* Due to the lack of security on the Internet it is inadvisable to transmit information without some sort of encryption. Gripman, *supra* n. 1, at 775. Consequently, if a business wants to use symmetric key encryption, it must either transmit the information over the Internet, at the risk of another party receiving the information, or engage in a face-to-face dialogue to ensure that no one

asymmetric key cryptography produced the digital signature.[22] While

intercepts the key. *Id.* At the point that a business picks up the telephone, uses the postal mail, or has a face-to-face meeting, whatever potential business advantage the Internet offers a company has been lost.

22. Thomas, *supra* n. 16, at 1010. This is a method of encryption created in 1978 by Ronald Rivest, Adi Shamir, and Leonard Adleman in which encoding and decoding a message is no longer dependent on the use of the same key but on the use of two mathematically related keys. *Id.* This is referred to as the "RSA method." *Id.* The RSA method is the most powerful and widely used asymmetric key cryptography system on the Internet. Gripman, *supra* n. 1, at 776. Asymmetric key cryptography uses two keys; one is private, the other key is public. *Id.* These keys are called a private-public key pair because they are mathematically linked to each other. *Id.* The two keys are linked such that if one key encrypts a message, the other key decrypts the message. *Id.* Asymmetric key cryptography does not pose the same security risk as does symmetric key cryptography because the parties use keys that are mathematically related but not the same. Thomas, *supra* n. 16, at 1010-11. The complexity of the mathematically related keys ensures that no one can reverse engineer one key to decipher the algorithm of the other. *Id.* at 1012. With algorithms serving as the essential component in the manipulation of data and the changing of information from text to digits, these algorithms are the foundation of asymmetrical cryptography. Lupton, *supra* n. 15, at ¶ 11. The RSA system creates two number parts of the encryption that creates a private-public key pair. Thomas, *supra* n. 16, at 1010. The first number comes from the encoding process; the second number is the product of a random mathematical computation and becomes part of the public key. *Id.* Another method of creating a digital signature is called "hashing." Like RSA, hashing also employs the use of an algorithm. Lupton, *supra* n. 15, at ¶ 11. Using the algorithm means if any of the characters change in a digitally signed message, the string of characters changes and produces a new, different a series of characters. *Id.* For example, the sender composes a message and runs it through a "one way hashing function"—an algorithmic function that takes the original message and creates a unique message digest. Gripman, *supra* n. 1, at 777-78. Each digest—the string of characters—is created in a fixed length that is small enough "to be enciphered as the message substitute in the construction of the actual digital signature with the private key." Lupton, *supra* n. 15, at ¶ 11 This allows for large plain text messages to be represented as the digital signature formation in a short string known to the user's encryption software. *Id.* Because hashing is a mathematical function, if any part of the digitally signed message were changed, the program would create a different message digest. *Id.* Accordingly, each message digest is unique to the original message. *See* Gripman, *supra* n. 1, at 778. Next the sender will encrypt the message digest with his private key, attach the original, unencrypted message, and send to the recipient. *Id.* For the recipient to decipher the information and to verify the digital signature, he must be familiar with the hashing algorithm of the sender. *Id.* The recipient must first down oad the sender's public key to decode the accompanying message digest. *Id.* To verify the message, the hashing algorithm must be applied to the plain text message that was sent; so, the recipient will take the original unencrypted message that the sender also sent and run that through the hashing function to produce a second message digest. *Id. at* 779. If there is a change in the digitally signed message, there is a corresponding change in the digest that causes a failure of the verification process. *Id.* On the other hand, verification of the message occurs when the second message digest is exactly the same as the first message digest. *Id.* Additionally, an unauthorized third party cannot take the digital signature from one document and affix it to another document because each digital signature is unique to a specific document. *Id.*

some state laws were similar to the Utah Act,[23] other state laws were fundamentally different from the Utah Act.[24] These states passed laws that protected not just digital signatures, but signatures that satisfied a criteria set forth in technology neutral statutes.[25] Instead of giving legal effect to a specific technology, technology neutral statutes provide legal protection for digital signatures or electronic signatures if they comply with the statutory criteria.[26]

By protecting electronic signatures only if they satisfy certain statutory criteria, California's statute is an example of technology neutral or "attribute legislation" as it has also come to be known.[27] One of the benefits of the legislature, was that businesses could use other types of digital signature technology, which may be less expensive and less complicated than public key encryption ("PKE").[28] In the event a cheaper digital signature technology comes along, the cheaper method

23. Smedinghoff, supra n. 5, at 741. States that passed legislation similar to the Utah Digital Signatures Act were Washington, Minnesota, Missouri, and New Hampshire. *Id.*

24. *Id.*

25. Utah Code Ann. § 46-3-401. A protected digital signature is one that was verified by the public key in a certificate issued by a licensed certification authority; the signature was affixed by the signer with the intention to sign the message; and the recipient does not have information that the signer is in breach of a subscriber agreement, presumably with the certification authority, or that the signer is not the proper owner of the private key. *Id.* § 46-3-401(a)-(c). Requiring the use of certification authorities or trusted third parties who use trustworthy systems to verify the authenticity of a transmission is another salient distinguishing feature of the Utah Act. *Id.* § 46-3-102(38).

26. Smedinghoff, *supra* n. 5, at 739 (providing citations for state digital signature statutes). Before state legislatures began implementing the UETA, well over one third of the states opted for digital signature legislation of this kind. *Id.*

27. Cal. Govt. Code § 16.5(a) (West 1999). Under the California Code, a digital signature had the same effect as a handwritten signature if five criteria were met. *Id.* The signature had to be unique to the person using the digital signature, capable of verification and under the sole control of the person using it; the date attached to the digital signature must be attached in such a way that if the date is changed the signature is invalidated; and had to conform to the rules and regulations established by the Secretary of State. *Id.* These five elements are not exhaustive because a governing body is free to determine the number and criteria that must be met to give legal effect to a digital signature. *E.g.* U.N. Comm. Intl. Trade L., Model Law on Electronic Commerce, 1996, Part I, Art. VII, subpara. 1 (a) - (b) [hereinafter UN Model Law]< http://www.uncitral.org/en-index.htm > (accessed July 17, 2000). The United Nations Committee on International Trade Laws ("UNCITRAL") has factors different from those in the California statute. *Id.* UNCITRAL requires that the digital signature must include a method to identify the signer; indicate the signer's approval of the information contained in the document; and "the method used was as reliable as was appropriate for the purpose for which the message was created or generated in light of all of the circumstances." *Id.*

28. Trusted third parties are places that act as a bank in holding the digital signatures. Kalama M. Lui-Kwan, *Recent Developments in Digital Signature Legislation and Electronic Commerce*, 14 Berkeley Tech. L.J. 463, 466 (1999). In fact, these trusted third parties, also known as certification authorities, can be a bank or company specializing in digital signature technology. *Id.*

must only satisfy the statutory conditions to receive the same legal status as a handwritten signature.[29] One more significant difference between California's signature legislation and Utah's is that California does not mandate the use of certification authorities or trusted third parties for the verification of a digital signature and the issuance of certificates.[30]

Another type of technology neutral statute is enabling legislation. Enabling legislation merely provides protection for electronic signatures without specifying that the signature must be the product of a certain technology or satisfy a set of statutorily defined criteria.[31] Enabling legislation can potentially cause significant problems because the legislation does not have the specificity of technology specific statutes.[32] For example, the Utah Act devotes significant attention to the creation, requirements, and functions of certification authorities and trusted third parties.[33] Enabling statutes, like that of South Carolina,[34] do not address, in detail, any issues relating to certification authorities and

29. Cal. Code Regs. tit. II, § 22002(a) (West 1999).

30. *Id.* While there is no mention of PKE and accepted technologies in the California Code, regulations supplement the Code with more specific information relating to the use of digital signatures and any other type of technology. Different from the Code, the regulations state that only accepted technologies may be used in producing digital signatures. *Id.* Acceptable technologies must be capable of creating a digital signature that is capable of satisfying the five factors set out in California Government Code section 16.5. *Id.* The regulations establish that "[t]he technology known as Public Key Cryptography . . . is an acceptable technology for use by public entities in California." Cal. Code Regs. tit. II, § 22003(a). Signature dynamics is another type of digital signature technology that is an acceptable technology under California law. *Id.* § 22003(b). Signature dynamics measures the characteristics of a signature on a flat surface and through the use of cryptographic techniques binds the measurements to the message. *Id.*

31. S.C. Code Ann. §§ 26-5-10 *et seq.* (2000). Under the South Carolina Electronic Commerce Act, an electronic signature is "any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the party using it to have the same force and effect as a manual signature." *Id.* § 26-5-30(4). A broader law is the Illinois Act which states that any record generated, communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another satisfies any law requiring a writing or a written record. *See* 5 Ill. Comp. Stat. § 175/5-105 (2000). Under the Illinois Act, the definition of electronic signature is broad enough to encompass both digital signatures and electronic signatures. *Id.* Unlike South Carolina's law, the Illinois Act gives increased legal protection for signatures classified as secure electronic signatures, which are signatures that can be verified by using a qualified security procedure. *Id.* § 175/10-110(a). A qualified security procedure is one that either party agreed upon or was approved by the Illinois Secretary of State. *Id.* § 175/10-110(a)(1)-(3). The criteria the Illinois Secretary of State uses is roughly similar to the criteria used by the California Secretary of State. *Compare* Cal. Govt. Code § 16.5(a) *with* 5 Ill. Comp. Stat. § 175/5-110(a)(1)-(3).

32. *Compare* S.C. Code Ann. §§ 26-5-30 *et seq. with* Utah Code Ann. §§ 46-3-101 *et seq.*

33. *Id.* § 46-3-104; *see generally* R. Jason Richards, *The Utah Digital Signature Act as "Model" Legislation: A Critical Analysis*, 17 John Marshall J. Computer & Info L. 873

trusted third parties.[35] Moreover, enabling legislation does not even carry the detail of the California legislation.[36] It is true that the California laws do not carry as much specificity as technology specific legislation, but at least California provides a list of specific criteria that digital signature methods must follow in order to receive legal protection.[37] Under enabling legislation, anyone signing their name or mark to a transmission receives full legal protection so long as there is an intention to sign.[38] The broadness of enabling statutes makes them untenable in addressing the concerns of e-commerce users because there is very little security for businesses.

The net result of this collage of state signature legislation was a confusing web of digital and electronic signature laws sprawling virtually across the entire country.[39] Compounding this problem is the universal nature of the Internet and e-commerce. If digital signature laws in Utah are different from those in South Carolina, then what law applies if a South Carolina company is conducting business with a customer in Utah? Attempting to harmonize business practices with a variety of state laws will certainly increase the transaction costs of e-businesses, which will effectively drive smaller businesses from the global marketplace.[40] Imagine if a South Carolina business had to familiarize itself with all of the nuances of the state signature laws of its potential customers. The cost would be prohibitive to a small company and very likely to a large one as well. Furthermore, a company would certainly be unable to engage in business activities with any meaningful celerity if they took the time to address these nuances. To resolve these issues, the federal government passed the Electronic Signatures in Global and National Commerce Act ("E-Sign").[41]

(1999) (discussing the many provisions of the Utah Act addressing certification authorities).

34. S.C. Code Ann. . §§ 26-5-10 *et seq.*

35. *See* Lupton, *supra* n. 15, at 15 (stating PKE can only be successful if there is a trusted third party to link the holder of an encryption key to an actual person).

36. *Compare* S.C. Code Ann. . §§ 26-5-10 *et seq. with* Cal. Code Regs. tit. II, § 22002(a).

37. Cal. Code Regs. tit. II, § 22002(a).

38. Smedinghoff, *supra* n. 5, at 741-42.

39. *See* President William Jefferson Clinton, Speech, *Electronic Signatures in Global and National Commerce Act* ¶ 8 (Washington, D.C., June 30, 2000) (available on Westlaw 2000 WL 1279512 (Leg. Hist.)) (claiming that the new federal legislation will provide legal certainty for businesses to invest in and expand e-commerce).

40. For example, imagine what would happen if the two employees of Sneech.com had to spend their time tailoring their transactions with customers so that each transactions conformed to the state law of each customer. Surely, this would stretch the human resources of Sneech.com to the breaking point and, at the very least, eliminate the efficiency offered by online transactions.

41. *Electronic Signatures in Global and National Commerce Act*, 15 U.S.C. §§ 7001 *et seq.* (2000). National Conference of Commissioners for Uniform State Laws ("NCCUSL")

E-Sign attempts to establish uniformity and clarity in the area of electronic signatures and electronic records.[42] Congress also intended that E-Sign would promote the use of electronic signatures and electronic records while avoiding the creation of a regulatory structure that would stifle the growth of e-commerce.[43] Continued growth of e-com-

---

established a wide consensus on what is necessary to eliminate the unintended impediments to e-commerce while not overriding laws that create the necessary requirements for the validating electronic signatures. H.R. Subcomm. on Cts. and Intell. Prop., *Hearing on H.R. 1714, Electronic Signatures in Global and National Commerce Act*, 106th Cong. ¶ 5 (Sept. 30, 1999) (Testimony of Pamela Meade Sargent, Commissioner for the NCCUSL) [hereinafter Sargent Testimony]. UETA was written over a two year period by NCCUSL under two guiding principles. *Id.* at ¶ 4. First, all solutions must be technology-and-business-model neutral. *Id.* at ¶ 5. Second, UETA only creates a framework for electronic commerce, meaning that there will be no displacement of a jurisdiction's applicable substantive law of or the creation of a new regulatory regime. *Id.* UETA interacts with existing state laws to assure that the results of transactions do not vary solely on the basis of the technology selected by the transacting parties. *Id.* at ¶ 18. Primarily, E-Sign and UETA provide three things: (i) an electronic signature or electronic record cannot be denied legal enforcement solely because they are electronic; (ii) if the law requires a writing, use of an electronic record satisfies the law; and (iii) if the law requires the use of a signature, use of an electronic signature satisfies the law. *Compare* 15 U.S.C. § 7001 *with* U.E.T.A. § 7 (1999).

42. H.R. Rpt. 106-341(I), Purpose and Summary at ¶ 1 (Sept. 27, 1999) (stating that the purpose of the legislation was "to facilitate the use and acceptance of electronic signatures and records in interstate and foreign commerce"). In addition to the morass of state digital signature legislation that created the need for federal legislation, some argue that this need for uniformity initially came about roughly two decades ago when U.S. businesses first began using electronic data interchange to contract for the very first time. Robert A. Witte & Jane K. Winn, *E-Sign of the Times*, ¶ 3 <http://www.kl.com/PracticeAreas/Technology/pubs/page20.stm> (accessed Feb. 10, 2001). With electronic data interchange, automated electronic contracting systems eliminated the need for employees to communicate with other consumers or businesses via traditional means, such as telephone, telexes. *Id.* In short, the creation of and subsequent reliance on electronic data interchange parallels the concerns over e-commerce in that companies that have a pre-existing relationship can easily reduce agreement to a writing, but significant issues arose when there was communication between parties absent a preexisting relationship. *Id.*

43. H.R. Rpt. 106-341(I), *supra* n. 42, Background and Need for Legislation at ¶ 11 (Sept. 27, 1999). "The legislation is narrowly drawn so as to remove barriers to the use and acceptance of electronic signatures and electronic records without establishing a regulatory framework that would hinder the growth of electronic commerce." *Id.*, Purpose and Summary at ¶ 1. Congress believed that the greater predictability and certainty embodied in E-Sign would nurture the continued growth of e-commerce. *Id.*, Background and Need for Legislation at ¶ 12. The lack of uniformity of electronic signature legislation not only has an effect on the U.S. e-economy but also on American businesses competing abroad and the ability of American businesses to remain at the forefront of business development. H.R. Subcomm. on Cts. and Intell. Prop., *Hearing on H.R. 1714, Allowing Use of Electronic Signatures*, 106th Cong. at ¶ 10 (June 9, 1999) (testimony of Jeffery Skogen, Internet Market Manager for the Credit Department of Ford Motor Company) [hereinafter Skogen Testimony] (finding that the lack of uniform nationwide rules may inhibit our country's ability to influence developments beyond its borders).

merce notwithstanding,[44] another benefit to e-businesses is greater legal certainty and predictability in their transactions.[45] Principally, E-Sign ensures that no signature or record will be denied legal effect because it is in electronic form.[46] E-Sign broadly defines electronic signatures as "an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[47] PKE is a process logically associated with a record and indicates an intent to sign; consequently, the broad definition of electronic signature applies equally to PKE.[48] Unlike state legislation, not only does E-Sign give general protection to parties using electronic signatures, but also provides specific provisions in the area of consumer protection.[49]

---

44. H.R. Subcomm. on Cts. and Intell. Prop., *Hearing on H.R. 1714, Allowing Use of Electronic Signatures*, 106th Cong. at ¶ 4 (June 9, 1999) (testimony of David Peyton, Director of Technology Policy of the National Association of Manufacturers) [hereinafter Peyton Testimony]. Business-to-business transactions account for far larger e-commerce transactions than consumer sales, and legal uncertainty and nonconformity force firms to use paper contracts for interstate commerce precluding complete automation. *Id.* at ¶ 7.

45. *Id.* at ¶ 11 (indicating that a uniform laws will allow businesses to fully automate their transactions to the point where industry would save billions). Interestingly, Congress understood that NCCUSL spent years struggling with the best way to fashion a model law that would create the uniformity and certainty that was necessary. *See e.g.* H.R. Rpt. 106-341(II), Purpose and Summary at ¶ 4 (Oct. 15, 1999). Yet, the fear that all 50 states would not adopt UETA and thus would still create a lack of uniformity in the law compelled Congress to continue its work with E-Sign. *Id.* (finding that the lack of uniformity and certainty still poses a barrier to the growth of e-commerce). It is interesting to note that in the September 27, 1999, report Congress suggested that the failure of half of the states to adopt UETA would be problematic in achieving the goals of uniformity and certainty but in the October 15, 1999, report Congress believed that anything short of adoption of all states would be anathema for uniformity and certainty. *Compare* H.R. Rpt. 106-341(I), *supra* n. 3, Background and Need for the Legislation at ¶ 12 *with* H.R. Rpt. 106-341(II), 42, Purpose and Summary at ¶ 4.

46. 15 U.S.C. § 7001(a). There are four things that E-Sign protects: (i) an electronic record or an electronic signature cannot be denied legal effect solely because they are in electronic form; (ii) if the law requires a writing, use of an electronic record satisfies the law; and (iii) if the law requires the use of a signature, use of an electronic signature satisfies the law. *Id.* UNCITRAL Model Law on Electronic Commerce has a rather significant influence on the provisions of E-Sign as well as UETA, for that matter. *See generally* UN Model Law, *supra* n. 28.

47. 15 U.S.C. § 7006(5).

48. *See id.* E-Sign is different from state technology neutral statutes in that most of the state technology neutral statutes usually have a list of accepted technologies in which PKE was included; E-Sign has no separate provision. *Compare* Cal. Govt. Code § 16.5(a) *with* 15 U.S.C. § 7006(5). The broad definition of an electronic signature encompasses technologically produced digital signatures and signatures as simple as a person typing their name at the bottom of an e-mail.

49. *Id.* § 7001(c). Consumers have the right to elect to receive electronic records in lieu of receiving a written record if two conditions are met. First, the consumer must affirmatively consent to receive the electronic record and has not withdrawn his consent. *Id.*

During the legislative development of E-Sign,[50] Congress was acutely aware of the need to respect state law and the processes of the "NCCUSL."[51] As E-Sign was originally written, it was believed that draft legislation placed stringent limitations on a state's ability to alter the effect of the federal legislation.[52] Many of the critics of the earlier preemption provision argued that if a state adopted UETA, the state would still be subject to the provisions of E-Sign to the extent that the state did not meet a number of ill-defined criteria.[53] Taking this concern to heart, Congress reexamined the bill during two mark-up sessions.[54] As a result of these mark-up sessions, the preemption provision was extended to UETA as reported to the state legislatures by NCCUSL.[55] Congress had several concerns: first, that a substantial number of states would not adopt UETA in a short period of time, and, second, that some states would not follow UETA and would develop their own standards for accepting electronic signatures that might not be compatible with UETA.[56] A compromise was to allow E-Sign to be the law until a state passed UETA, at which point E-Sign would expire.[57] Unfortunately, the House of Representatives did not accept this compromise and passed H.R. 1714, which was modified by the Conference Committee and subse-

---

§ 7001(c)(1). In order for the consumer to show affirmative consent to receiving the record electronically, there must be a reasonable demonstration that the consumer will be able to receive the electronic record to which consent is given. *Id.* The second condition is that prior to giving consent, the consumer must be provided a clear and conspicuous statement notifying him of his rights and options to have the electronic record made available on paper and the right to withdraw consent for receiving the records electronically. *Id.* § 7001(c)(1)(B). The statement must contain information notifying the consumer of any right he has to receive the record on paper or other non-electonic form; the procedures the consumer must use to withdraw consent or to update his electronic address; whether the consent is for information relating to a single transaction or categories of information or records that may be provided during a relationship; how the customer may request a paper copy of any electronic record; and the hardware and software requirements necessary for accessing electronic documents. *Id.* § 7001(c)(1).

50. The House version of the E-Sign was H.R. 1714, and the Senate's version was S. 761. Thomas E. Crocker, *The E-Sign Act: In Facilitation of E-Commerce*, 3 Cyber Tech Litigation Report 1, 4 (2001).

51. *Id.* at 22.

52. H.R. Subcomm. on Cts. and Intell. Prop., *Hearing on H.R. 1714, Allowing Use of Electronic Signatures*, 106th Cong. at ¶ 18 (Sept. 9, 1999) (testimony of Andrew J. Pincus, General Counsel for the U.S. Department of Commerce [hereinafter [Pincus Testimony]).

53. *Id.* at ¶ 19.

54. Crocker, *supra* n. 50, at 11.

55. *Id.*

56. *Id.*

57. *Id.* Congressional leaders even attempted to amend the bill with a substitute measure that was based on the compromise in the Senate bill S 761, which would have not recognized the preemption of state law. *Id.*

quently passed by both the House of Representatives and the Senate.[58]

III. ANALYSIS

Under U.S. law, federal statutes can either mutually co-exist with relevant state laws or the federal laws can supersede the state law.[59]

A. State Law and the Ability to Preempt E-Sign

There are three conditions that will cause the federal law to preempt a state law. First, a federal law preempts state law if the federal law contains language expressly preempting state law.[60] While E-Sign has an effect that may be classified as preemptive, there is nothing in the federal statute to indicate an express preemption of state law,[61] other than those statements contained in section 7002 of E-Sign.[62] Furthermore, Congress did not draft E-Sign with such specificity and depth that would give rise to a preemptive effect.[63]

Second, if the federal law governs the entire field of activity, it will preempt state law.[64] Federal statutes that seek to occupy the entire

58. The proposed compromise of the Senate was more favorable for two reasons. First, the Senate version did not preempt state legislation addressing electronic signatures that was consistent with section 6(a), prohibiting the denial of a contract because an electronic signature or electronic record was used in its formation, and Section 6(b), allowing the parties to determine the technologies or business models they wish to use, of S. 761. Crocker, *supra* n. 50, at 5. Second, a state did not have to enact the final version of UETA without modification or amendment. *Id.* The Senate bill allowed for the state version of UETA to receive protection if the states enacted UETA substantially as reported to the state legislatures by NCCUSL. *Id.*

59. *Compare* 15 U.S.C. §§ 101 *et seq.* (2000) *with* 15 U.S.C. § 1012(b) (prohibiting federal courts from construing a federal statute that would invalidate, impair, or supercede state laws involving insurance regulation); *see also First Nat. Bank in Plant City v. Dickinson*, 396 U.S. 122, 130 (1969) (reasoning that federal law regarding national bank branches does not preempt state laws governing the operation of national branches). Section 301 of the Copyright Act abolishes common law in the area of copyright by eliminating the 1909 Copyright Act's dual federal and state copyright protection and creates stringent standards that must be met before the federal law preempts state law. *See* 15 U.S.C. § 301(a).

60. 15 U.S.C. § 301; *see Shaw v. Delta Air Lines, Inc.*, 463 U.S. 85, 95-98 (1983).

61. *See e.g.* 15 U.S.C. § 7002(a).

62. Raymond T. Nimmer, *Electronic Signatures and Records, A New Perspective*, 17 Computer & Internet L. 8, 19 (2000).

63. *Id.* When Congress attempts to preempt a field of law that has traditionally been occupied by the states, congressional intent to displace a state law in that field must be clear and manifest. *Jones v. Rath Packing, Co.*, 430 U.S. 519, 525 (1977). E-Sign must have a provision that clearly expresses the intent of Congress to preempt applicable state laws. Presumably, these clear and manifest testaments of congressional intent must be within the statute itself and not merely in the legislative history, which is not the law.

64. *English v. General Electric, Co.*, 496 U.S. 72, 78-80 (1990); *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947) (stating that preemption also occurs where an act of Congress "touches a field in which the federal interest is so dominant that the federal sys-

field, such as the federal Bankruptcy Code or the Copyright Act, are typically far more extensive in their coverage of topics within the field.[65] The very nature of E-Sign suggests that Congress did not intend for E-Sign to occupy the entire field.[66] E-Sign is a statute of a very narrow scope which does not cover all of the legal areas relating to electronic signatures.[67]

Finally, if a state law will frustrate and conflict with a policy objective of federal law, the federal law preempts state law.[68] The policy objective of E-Sign is to promote e-commerce by providing: that electronic signatures and electronic records are legally sufficient;[69] consumer pro-

---

tem will be assumed to preclude enforcement of state laws on the same subject"); *but see Cipollone v. Liggett Group, Inc.*, 505 U.S. 504 (1992) (stating that matters outside of the preemptive reach of Congress are not preempted).

65. Nimmer, *supra* n. 62, at 20.

66. *Id.* Because the policy of E-Sign is that a requirement in law that a contract be signed can be met by an electronically signed contract, E-Sign can be classified as a narrow statute that does not attempt to occupy the entire field of transactions, although an argument can be made that E-Sign is an attempt to occupy the entire field. Focusing on the concept of "the field," one can argue that people asserting that E-Sign does not occupy the field assume that the relevant field is contracts or transactions. However, those arguing that E-Sign does occupy the field see the field as electronic contracting. Clearly, E-Sign is an attempt to occupy the field of electronic contracting. E-Sign's raison d'etre was the potpourri of state legislation that hindered the growth of e-commerce. Congressional statements regarding the purpose of E-Sign speak to the need and the desire to create uniformity and certainty in order to promote e-commerce and to increase consumer comfort with electronic transactions. It seems counter-intuitive for Congress to respond to the need for uniformity and legal certainty by creating a law that that does not occupy the entire field. The argument that E-Sign is not as extensive as the Bankruptcy Code and therefore does not occupy the field is specious for two reasons. First, for a myriad of reasons, one being the creation and explosion of e-commerce within the past six years, issues relating to electronic contracting are very limited, or, at the very least, not as numerous as those presented by bankruptcy or copyright. Consequently, a law relating to electronic contracting will be, by comparison, less extensive than those areas that have their roots in the common law of England. Second, these fundamental differences between electronic contracting and bankruptcy make comparing the extensiveness of their respective statutes futile. There are, however, enough areas within electronic contracting to find that E-Sign was not meant to occupy the entire field. As previously discussed, E-Sign's broad definition of electronic signature includes digital signatures. It is common that many technology-specific statutes impose insurance requirements or registration requirements on certification authorities. These areas are not covered in any provision under E-Sign but have been addressed in some state digital signature laws. *See e.g.* Utah Code Ann. § 46-3-104.

67. Nimmer, *supra* n. 62, at 20.

68. *Florida Lime & Avocado Growers, Inc. v. Raul*, 973 U.S. 132, 142-143 (1963) (finding federal preemption where it is impossible for a private party to comply with the state and the federal requirements); *Hines v. Davidowitz*, 312 U.S. 52, 57 (1941) (arguing that preemption occurs where a state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.").

69. 15 U.S.C. § 7001(a).

tections;[70] requiring the retention of and access to electronic records;[71] guidelines for the notarization of electronic transactions;[72] and provisions relating to the business of insurance, insurance agents and brokers.[73] If a state law conflicts with these provisions of E-Sign, the state law will fall to E-Sign's preemptive effect. However, there is little evidence in E-Sign to suggest that its preemptive effect applies to state signature laws falling outside of the policy objectives of E-Sign.[74]

E-Sign does not have a preemptive effect for state signature laws falling outside of the provisions articulated in section 7001. However, E-Sign's preemption functions in a very unique manner because there are two conditions under which a state can exercise control over E-Sign.[75] However, there are two provisions that must be addressed when considering whether a state law has been preempted by E-Sign. The first provision is section 7002(a)(1), and section 7002(a)(2) is the second provision.

B. The Clean Version of UETA

A state can pass a statute, regulation, or other rule of law that modifies, limits, or supersedes the provisions of section 7001 of E-Sign.[76] Section 7002(a)(1) provides that any state statue, regulation, or other rule of law must be an enactment or adoption of UETA as approved by NCCUSL.[77] However, section 7002(a)(1) provides that any exemptions to the state version of UETA made under UETA section 3(b)(4) is preempted to the extent it is inconsistent with Title I or,[78] Title II,[79] or not

---

70. *Id.* § 7001(c).

71. *Id.* § 7001(d).

72. *Id.* § 7001(g).

73. *Id.* § 7001(i)-(j).

74. Nimmer, *supra* n. 62, at 21.

75. *See id.*, at 21-22. Professor Nimmer finds E-Sign's preemption provision unique and curious because no federal statute has a provision that functions in the same manner as E-Sign's. *Id.*

76. 15 U.S.C. § 7002.

> A State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of section 7001 with respect of state law only if such State statute, regulation, or other rule of law constitutes an enactment or adoption of the Uniform Electronic Transaction 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 shall be preempted to the extent such exemption is inconsistent with the title or title II, or would not be permitted under paragraph (2)(A)(ii) of this subsection.

Id. § 7002(a)(1). Interestingly, the House of Representatives included a provision that the states had to enact UETA within four years from the enactment of E-Sign. *See* H.R. Rpt. 106-341(1), *supra* n. 42, Section-by-Section Analysis of the Legislation at ¶ 8.

77. 15 U.S.C. § 7002(a)(1).

78. *Id.* §§ 7001 *et seq.*

permitted under section 7002(a)(2)(A)(ii).[80]

Section 7002(a)(1)'s cross-reference to subsection (a)(2)(A)(ii) is very important.[81] The insertion of the cross-reference means that if a state passes UETA with 3(b)(4) exemptions, the exemptions cannot afford greater legal status to a specific technology or technical specification for electronic signatures.[82] Given that section 7001(a)(1) states that E-Sign preempts UETA Section 3(b)(4) exemptions to the extent they are inconsistent with Titles I and II, does this mean that the rest of the exempted law remains in force? Or does it mean that E-Sign preempts the entire exemption? The language of the statute suggests that the conflicting part of the exemption will be preempted because E-Sign preempts "to the extent" the exemption is "inconsistent with" the provisions of E-Sign.[83]

Some commentators suggest that any modification or amendment to UETA means that E-Sign preempts UETA.[84] On the other hand, there are those who argue that there must be more than a de minimus modification, alteration, or amendment before E-Sign preempts UETA.[85] Failure to be mindful of E-Sign's objectives leads to the erroneous conclusion that E-Sign should only preempt the state version of UETA when the modifications or amendments are material. First, the principal purpose

79. *Id.* § 7021. This section provides the criteria for addressing electronic negotiable instruments. Primarily, these provisions address the creation, transferability, and enforceability of holding electronic notes against the issuer or the obligor. *Id.* The specifics of this provision are outside of the scope of this comment and will not be discussed in detail. Section 7021, however, will be referred to in this comment as Title II.

80. *Id.* § 7002(a)(1). This provision is critical because it closes a loophole in UETA. UETA section 3(b)(4) allows a state to exempt specific transactions from the state version of UETA so long as there is a state law governing a particular transaction. U.E.T.A. § 3(b)(4) (stating that UETA does not apply to "other laws . . . identified by the State"). There is evidence to suggest that NCCUSL saw section 3(b)(4) as a catch all provision for exemptions because the "[d]rafting Committee recognized that some legislatures may wish to exclude additional transactions from the Act." *Id.* at 3(b)(4) cmt. 9. The Drafting Committee provides guidance as to whether or not a state should use the 3(b)(4) exemption for certain types of transactions. One of the areas addressed by the Drafting Committee is consumer protection laws. While the comment suggests that a state legislature should not use the section to exempt consumer protection provisions, these comments only provide guidance and, thus, are not legally binding. Consequently, it is possible, without section 7002(a)(1), for a state to exempt from UETA laws requiring the disclosure of certain information.

81. 15 U.S.C. § 7002(a)(1).

82. *Id.*

83. *Id.*

84. Nimmer, *supra* n. 62, at 17. Professor Nimmer argues that the state enactments of UETA must be clean ie., free of modification and amendments. *Id.* The change could be as minor as an alteration of a definition or as significant as a modification of any of UETA's provision, such as the consumer consent provisions. Under E-Sign's section 7002(a)(1) any change to the final version of UETA will invalidate the modified state version of UETA and allow E-Sign to remain in effect. *Id.*

85. Crocker, *supra* n. 50, at 23.

for creating a federal law was to give a uniformity, predictability, and legal certainty as opposed to the previous legal regime where laws differed from one state to the next.[86] Also, allowing states to make minor variations to UETA creates a lack of uniformity that would be no better than the previous state-based regime. Even under the new regime, businesses and consumers would still be left with a framework that potentially varies from state to state. Second, section 7002 contains a limiting instruction that seems to suggest that only exemptions that are inconsistent with E-Sign or prohibited under subsection 7002(a)(2)(ii) would be preempted.[87] This means that E-Sign already provides a state the flexibility to make minor modifications to a state version of UETA.[88] Accordingly, there is no need to loosely interpret section 7002(a)(1).

Section 7002(a)(1) provides another alternative for a state seeking to escape federal legislation.[89] This provision could be interpreted to mean that E-Sign will not preempt state law if the law is either an enactment of the NCCUSL-approved version of UETA or the law is not a NCCUSL-approved version of UETA but is technology neutral.[90] Only a very close reading of section 7002(a)(1) leads to this conclusion, and admittedly, the close reading relies very heavily on interpreting the placement or misplacement of a comma.[91] However, such a reading would create a loophole while closing UETA's Section 3(b)(4) loophole.[92] A close reading would allow for flexibility in making changes to UETA that are not substantive.[93] The technology that supports the digital revolution rapidly changes and evolves to the point where different challenges arise. Flexibility to make nonsubstantive changes to UETA may provide the steady

86. *Compare* S.C. Code Ann. §§ 26-5-30 *et seq.* (enabling legislation) *with* Utah Code Ann. §§ 46-3-101 *et seq.* (creating a technology-specific regime in Utah).

87. *See* 15 U.S.C. § 7002(a)(1). Section 7002(a)(1) provides 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 title or title II, or would not be permitted under paragraph (2)(A)(ii) of this subsection." *Id.*

88. Under E-Sign, if a state passes a version of UETA that contains modifications or amendments, the state is not adopting the final version of UETA as proposed by NCCUSL as required by section 7002(a)(1). However, the state can then use section 7002(a)(2). If the state version of UETA is consistent with the provisions of 7002(a)(2), the state version of UETA supersedes E-Sign.

89. *Id.*

90. Crocker, *supra* n. 50, at 23.

91. *Id.* at 23. Here is where legislative history would be a great asset. Unfortunately, the conference report of H.R. 1714, the House version of E-Sign, is merely a restatement of the text of the bill without the supporting or clarifying statements of the managers of the bill. *Id.* at 12. This means that there is no authoritative legislative history. Consequently, there is no guidance as to whether section 7002(a)(1) should be interpreted broadly or narrowly. *Id.*

92. *Id.*

93. *Id.*

framework that is necessary for wide spread use of digital and electronic signatures.[94]

In order to determine whether or not E-Sign preempts state laws, a person must examine the laws on a state-by-state basis. A business must decipher whether a state adopted UETA, and if the State did adopt UETA, does the state version contain 3(b)(4) exemptions. If a business determines that a state version of UETA does in fact contain 3(b)(4) exemptions, the business must make a determination as to whether the exemptions are consistent with Titles I and II of E-Sign. If the business determines that the exemptions are inconsistent with Titles I and II, then E-Sign preempts. Yet, it is uncertain whether E-Sign preempts the entire exemption or only those provisions which are inconsistent with Titles I and II. Remember that we are uncertain whether the final provision in section 7002(a)(1) means that the state version of UETA must, in addition to being consistent with Titles I and II, also be technology neutral or whether the state version must be either consistent with Titles I and II or be technology neutral. A business has to make several educated guesses as to the meaning of the laws. The above assumes that the state has adopted a clean version of UETA—one that has no alterations, amendments, or modifications.

Despite the confusion section 7002 poses, there are some parts that afford clear answers. Several parts are self-evident. If a state adopts a clean version of UETA, the state version of UETA replaces E-Sign and is valid and enforceable. If a state passes a clean version of UETA and uses UETA's section 3(b)(4) to exempt the same laws that are exempted under E-Sign,[95] E-Sign will not preempt these exempted provisions because they are not inconsistent with Title I of E-Sign.

---

94. Remember that under the Illinois Act, an electronic signature receives legal effect if it meets the standards that are substantially similar to those delineated in the California statute. Cal. Code Regs. tit. II, § 22002(a). Yet, the Illinois Act goes farther than other attribute-legislation statutes because it affords greater legal protection to electronic signatures and records that are the either secured electronic records or secured electronic signatures, which are records or signatures that are verified by using a secured system. 5 Ill. Comp. Stat. § 175/10-110(a)(1)-(3).

95. E-Sign exempts state laws relating to

> (1) a statute, regulation, or other rule of law governing the creation and execution of wills, codicils, or testamentary trusts;
> (2) a State statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; or
> (3) the Uniform Commercial Code, as in effect in any State, other than sections 1-107 and 1-206 and Articles 2 and 2A.
> (b) Additional exceptions. The provisions of section 101 [*15 USCS § 7001*] shall not apply to—
> (1) court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings;
> (2) any notice of—

If, however, the state exempts laws that go beyond the reach of E-Sign's exemptions, E-Sign preempts those laws because they are modifications that are inconsistent with Title I. For example, a state provision exempting insurance brokers from the signature provisions would be preempted by E-Sign because Congress intended for the provisions of Title I to apply to the business of insurance.[96] Consequently, exempting the business of insurance from the state version of UETA is a modification that is inconsistent with Title I, and thus preempted. Preemption even occurs when a state passes a clean version of UETA and exempts a law under section 3(b)(4) that does not contain consumer consent provisions. Such a law would be preempted because it too is inconsistent with Title I of E-Sign, which carries very clear and extensive consumer-consent provisions. Finally, if the state enacts a clean version of UETA that mandates the use of a particular technology, E-Sign preempts that provision as well because such a law, even if exempted under 3(b)(4) would fail the technology neutral provision of section 7002(a)(2).

C. State Law and Alternative Procedures

E-Sign allows states that decide, for whatever reason not to pass a clean version of UETA to create their own signature statutes.[97] But in order for the state's legislation to supersede the provisions of the federal legislation, the state statute must comply with the conditions articulated in subsection (a)(2).[98] First, the alternative procedures or requirements proposed by the state must be consistent with Titles I and II of E-Sign.[99] Second, the alternative requirements or procedures cannot give greater

(A) the cancellation or termination of utility services (including water, heat, and power);
(B) default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;
(C) the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or
(D) recall of a product, or material failure of a product, that risks endangering health or safety; or
(3) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

15 U.S.C. § 7003.

96. *Id.* § 7001(i)-(j).

97. *Id.* § 7002(a)(2).

98. It is important to note that E-Sign allows the states to pass legislation that does not have to comport with the provisions of section 7002(a)(2). Specifically, the technology neutral provision does not have to be satisfied if the state statute, regulation, or rule of law pertains to a state acting as a market participant—where the state competes in a market as if it were a private corporation. *Id.* § 7002(b). While section 7002(b) is an important provision, this comment will focus only on the effect of the preemption provisions contained in section 7002(a), and, thus, section 7002(b) is outside of the scope of this comment.

99. *Id.* § 7002(a)(2)(A)(i).

legal status to "the implementation or application of a specific technology or technical specification for performing the function of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures."[100] Finally, if the state enacts the alternative requirement after E-Sign's enactment, the alternative must specifically mention E-Sign.[101]

It is important to remember that the second provision also functions as a savings provision. If a state passes a version of UETA that has provisions that do not conform to E-Sign, the state's finding that their version of UETA does not fit into section 7002(a)(1) may attempt to validate the law using section 7002(a)(2)(A). Yet, while this can function as a savings provision, there is a potential problem. Section 7002(a)(1) has a provision addressing the UETA's section 3(b)(4) exemptions, but section 7002(a)(2) does not have a similar provision.[102] Consequently, this means that exemptions made under section 3(b)(4) of UETA fail section 7002(a)(2) because they are inconsistent with Title I of E-Sign,[103] and so too does the entire statute.[104]

So, how does section 7002(a)(2) function? If a state passes UETA with modifications, the law will not be preempted if the provisions are not inconsistent with E-Sign or are not technology specific. This should be the result regardless of whether the provisions of the state version of UETA conform with NCCUSL's version of UETA. Additionally, if a state passes a version of UETA that contains modifications and has section 3(b)(4) exemptions, the state version of UETA and the exemptions would be reviewed for consistency with E-Sign. Provisions that are either inconsistent with E-Sign or violate E-Sign's technology neutral requirement should cause the state version of UETA and the exemptions to be preempted.

These preemption clauses serve as a disincentive to engage in e-commerce because the question of what law applies still remains unanswered.[105] Essentially, E-Sign's preemption provision causes the entire statute to fall far short in achieving its essential function—to promote clarity and to promote uniformity of U.S. signature legislation.[106] The fact that section 7002(a)(1) addresses UETA's section 3(b)(4) exemptions

100. *Id.* § 7002(a)(2)(A)(ii).

101. *Id.* § 7002(a)(2)(B).

102. *Compare* 15 U.S.C. § 7002(a)(1) *with* 15 U.S.C. § 7002(a)(2).

103. Crocker, *supra* n. 50, at 25.

104. *Id.*

105. *Cf.* Sargent Testimony, *supra* n. 41 at ¶ 23. Only UETA, as adopted in state law, stands alone as the source of law of electronic records and signatures. *Id.* at ¶ 24.

106. *Id.* at ¶ 24-25 (noting that the preemption provision of E-Sign is very difficult to interpret). "One could make a serious argument that [15 U.S.C. § 7002(a)] encourages nonuniformity [sic] rather than uniformity." *Id.* at ¶ 25.

while section 7002(a)(2) does not is a major source of confusion. Additionally, there is no legislative history to assist in the interpretation of whether section 7002(a)(1) requires the state version of UETA to be consistent with Titles I and II and the technology neutral requirement, or whether the state version of UETA can survive section 7002(a)(1) analysis if it is either consistent with Titles I and II or technology neutral. Combining the lack of illustrative legislative history and a vagueness of these provision that borders on chaotic,[107] judicial interpretation is left as the only means of delineating the scope and application of E-Sign or state versions of UETA. However, allowing a state court or even a federal court to clarify something that is intrinsically obscure could lead to inconsistent common law.[108]

D. New Preemption Provisions

In order for E-Sign to promote e-commerce and business and consumer confidence in electronic transactions,[109] Congress should amend E-Sign.[110]

This comment suggests a method by which this may be accomplished. A possible solution is amending section 7002(a)(1) of E-Sign to read that all state statutes, regulations, or other rule of law must constitute:

> an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all States by the National

---

107. *Id.* at ¶24. Without further clarification, UETA and E-Sign section 7002(a) are a hybrid of field and subject preemption, which without further explanation leads to no predictable interpretation. *Id.*

108. It is not as if this is without precedent. In 1939, the Restatement of Torts created a definition of a protectable trade secret that is widely used in many state statutes. Linda B. Samuels and Byron K. Johnson, *The Uniform Trade Secrets Act: The States' Response*, 24 Creighton L. Rev. 49, 53 (1990). Because the Restatement of Torts failed to address such issues as the applicable statute of limitations and the availability of injunctive relief, many state courts had differing interpretations of the approach to trade secret protection. *Id.* Courts that addressed the misappropriation of trade secrets consistently relied on the Restatement of Torts as their source for the common law principles but interpreted the provision in different ways. Brandon S. Cate, *Saforo & Assoc., Inc. v. Porocel Corp.: The Failure of the Uniform Trade Secrets Act to Clarify the Doubtful and Confused Status of Trade Secrets Common Law Principles*, 63 Ark. L. Rev. 687, 695-696 (2000).

109. Clinton, *supra* n. 39, at ¶ 9-10. Companies will have the legal certainty they need to invest and expand in e-commerce by being able to purchase products and services and to potentially save billions by retaining records in electronic form. *Id.* at ¶ 9. Ironically, President Clinton also suggested that by not favoring one form of technology over another will "unleash the full potential of the digital economy." *Id.* at¶ 7.

110. *See e.g.* 15 U.S.C. § 7005(b). It is apparent what that one of the principal goals of E-Sign is the promotion of e-commerce. E-Sign requires that the Secretary of Commerce and the Federal Trade Commission file a report with Congress one year after the enactment of E-Sign addressing not only the benefits to the consumers but also the benefits to e-commerce. *Id.*

> 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) that is inconsistent with Titles I, Title II, or 7002(a)(2) is preempted in its entirety.[111]

The first problem that E-Sign must address is its relationship with UETA. Remember that the underlying purpose of both E-Sign and UETA is to create uniformity, predictability, and certainty of laws relating to electronic signatures and records.[112] The current version of E-Sign provides that it can be superseded by UETA if the state enacts UETA as approved by NCCUSL. However, confusion remains as to the extent of E-Sign's preemptive effect if a state makes minor modifications to UETA but retains its critical provisions. Moreover, there is confusion as to whether 3(b)(4) exemptions must be consistent with Titles I and II and be technology neutral. The new provisions make it clearly understood that any modification, de minimus or material, to UETA will cause the state's version of UETA to be preempted in its entirety.[113] For example, in California, the current version of UETA with all of its modifications and amendments would be preempted by E-Sign until California passes an unmodified version of UETA. Additionally, this new provision also addresses the confusion regarding the 3(b)(4) exemptions by requiring that the exemptions be consistent with Titles I and II of E-Sign and the new section 7002(a)(2). Making the exemptions consistent with Titles I and II of E-Sign is a sensible way to promote uniformity in exempted state laws. For states adopting the unamended and unmodified version of UETA, E-Sign should also clarify that its provisions are default provisions where terms or provisions conflict with UETA,[114] E-Sign

111. App., 15 U.S.C. § 7002(a)(1).

112. H.R. Rpt. 106-341 (II), *supra* n. 43, Background and Need for the Legislation at ¶ 2.

113. App., 15 U.S.C. § 7002(a)(1). One might be able to make the argument that a new provision should be more like the Senate version, S. 761, in that a state can pass a version of UETA that is substantially similar to the final version proposed in July 1999 by NCCUSL. The problem is that there is still the potential for a lack of uniformity. Under the Senate version, each state may make modification or amendments to UETA so long as the state version is substantially similar to the final version. First and foremost, there is no way to determine what changes can be made before a state version is no longer substantially similar. Second, if the states make different modifications and amendments to UETA, there will not be any consistency among the state versions of UETA. Adopting the Senate version will not address the lack of uniformity on the state level.

114. There are several provisions that UETA addresses that E-Sign either fails to address fully or even contemplate. E-Sign provides that contracts formed by one or more electronic agents cannot be denied legal effect. 15 U.S.C § 7001(h); *see* 15 U.S.C. § 7006(3) (defining electronic agent as "a computer program used independently to initiate or respond to electronic records without review by an individual at the time of the action"). UETA provides a little more specificity in the protection of contracts formed by the interaction of an electronic agent and an individual, who is acting on his own behalf or for another person. UETA § 14. UETA protects any interaction where "the individual performs actions that the individual is free to refuse to perform and which the individual knows or has

prevails.[115] However, an exception can be made in situations where there is a conflict and UETA provides greater protection than does E-Sign.[116]

Moreover, under the current system, a business has no idea if the current California version of UETA, or any other state version of UETA with amendments and modifications, applies, whether the amendments and modifications apply but the rest of UETA does, or if E-Sign applies.[117] Furthermore, a business would still likely find itself confronting the issue of trying to comply with different versions of UETA. An e-business now has to attempt to comply with California's UETA, which might be different from Virginia's version of UETA.[118] This problem is reminiscent of the pre-E-Sign days where a business had to be aware of the various types of state legislation and conducted business accordingly.[119] The new section 7002(a)(1) simplifies these considerations immensely. If a state has a version of UETA that has any modifications whatsoever, E-Sign is the applicable law, regardless of whether the modification is as minor as removing an adjective. If the state has a clean version of UETA, businesses and consumers can be assured that UETA applies. Most importantly, if a state has 3(b)(4) exceptions, one only needs to ask three questions. First, is the exemption consistent with Title I? Second, is the exemption consistent with Title II of E-Sign?

---

reason to know will cause the electronic agent to complete the transaction or performance." *Id.* § 14(2). Essentially, this provision states that agreeing to a click-through agreement falls within the provisions of UETA.

115. Nimmer, *supra* n. 62, at 23. One such area where E-Sign grants more protection than does UETA is in the area of consumer protection. *Compare* 15 U.S.C. § 7001(c) *with* U.E.T.A. § 5.

116. UETA addresses in great detail attribution, but E-Sign fails to cover this topic. U.E.T.A. § 9. A signature is attributable to a person only if it was performed by an act of that person. *Id.* § 9(a). The act of attribution can be shown in any manner, such as by the actions of human or electronic agents. *Id.* UETA, unlike E-Sign, also establishes specifications for how to determine when a document is sent or received. *Id.* § 15. Additionally, in an area that is not addressed at all in E-Sign, UETA provides guidelines for the effect of a message that has been changed during transmission. *Id.* § 10.

117. The California version of UETA adds provisions under the section entitled "Use of Electronic Records and Electronic Signatures," the notarization and acknowledgement section and the time and place of sending and receipt section. Additionally, the California version removes sections 16 through 20 of the NCCUSL version of UETA. Sections 16 through 20 in NCCUSL's version address transferable records and use of electronic records by government agencies. Cal. Gov't Code § 16.333.

118. Arizona, Arkansas, California, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kentucky, Maine, Maryland, Montana, Nebraska, New Mexico, Ohio, Oregon, Rhode Island, Utah, Vermont, Virginia, and West Virginia have enacted the final version of UETA but have also made additions or deletions to their versions which make the adopted state version different from the final version of UETA as proposed by NCCUSL.

119. For a discussion about the failure of state laws to create a uniform standard, review *supra* nn. 16-35 and accompanying text.

Third, is the exemption consistent with the new section 7002(a)(2)? If the answer to any of these questions is in the negative, E-Sign preempts the provision in its entirety. This uniformity and clarity creates another benefit for businesses and consumers—predictability. Under this new method, businesses will be able to fashion their business models and Web sites accordingly, and consumers can readily discern which statutory provisions apply. A provision causing E-Sign to become inapplicable if all of the states passed unmodified versions of UETA would avoid further complications.[120]

Another change for E-Sign would be to embrace the technical specifications for producing an electronic record or electronic signature—a new section 7002(a)(2).[121] It goes without saying that using either the public-private key method or the hashing method is inherently more secure in authenticating the other party and verifying the integrity of the document.[122] To promote this type of security, E-Sign, taking a page from the Illinois Act,[123] should give greater legal protection for those methods that afford a more reliable method of authenticating the party and the integrity of the transmission.[124] Legislation giving greater legal protections to PKE promotes the development of more PKE software.[125]

---

120. It has been suggested that E-Sign should be a federal law of limited duration. Pincus Testimony, *supra* n. 52, at ¶ 15 (stating that E-Sign should be limited to a temporary federal rule to ensure the validity of electronic agreements entered into before states enact the UETA). "Once the UETA is adopted by a State, the federal rule [E-Sign] would be unnecessary and should 'sunset'." *Id.*

121. App., 15 U.S.C. § 7002(a)(2) (prohibiting a state from providing greater legal effect to a particular method of affixing digital signatures). Allowing for greater legal protection for digital signatures produced by PKE is only one part of the process to help e-commerce reach its potential. Peyton Testimony, *supra* n. 44, at ¶ 8 (stating that "before electronic commerce can reach its full potential, business must be provided assurance that traditional signature law encompasses electronic authentication"). A party to an electronic transaction may use a variety of methods to evidence his identity or his agreement to the terms of a contract—"electronic authentication"—such as, a previously agreed code-word or with an electronic facsimile of his written signature created by an electronic stylus, a digital signature, or some biometric technology. Pincus Testimony, *supra* n. 52, at ¶ 06.

122. Gripman, *supra* n. 1, at 779. "Digital signatures using public key encryption technology enable parties to transact business over the Internet by verifying the identities of the parties and the integrity of the messages communicated." *Id.*

123. Under the Illinois Act, a secure electronic signature must satisfy three levels of scrutiny: an analysis of the security procedure; if the electronic record or document has been altered since a particular point in time; and if the electronic signature is a signature of a particular person. 5 Ill. Comp. Stat. §§ 175/5-105, 105(a), 110(a). In a civil matter, there is a rebuttable presumption that the electronic record has not been altered since the record went through the secure procedure. *Id.* § 175/10-120(a). In the case of electronic signatures, if the signature has gone through a secure process, the presumption is that the signature correlates to the person it represents. *Id.* § 175/10-120(b).

124. *See* Appendix 1.

125. Martin I. Behn, *The Illinois Electronic Commerce Security Act: Too Much Too Soon or Too Little Too Late*, 24 S. Ill. U. L.J. 201, 208 (2000). One of the arguments in support of

First, the new section requires alternative procedures or requirements to be consistent with Title I and Title II. This correlates with the new section 7002(a)(1). Moreover, this section also addresses a shortcoming of the original section by requiring that any 3(b)(4) exception attempting to find protection under this section must also be consistent with Titles I and II and the subsections of 7002(a)(2). Second, subsection (a)(2)(A)(ii) provides that the alternative procedure may give greater legal effect to electronic signatures that are the product of a specific technology.[126] Essentially, this provision is a complete reversal of the former version of 7002(a)(2)(ii) in that there is no technology neutral requirement. Technology specific procedures only receive legal protection if by using a qualified security procedure,[127] it can be verified that an electronic signature is the signature of a specific person.[128] There is no reason why methods that allow for greater accuracy in authentication and verification of message integrity should receive the same legal protection as a person typing their name at the bottom of an electronic purchase order.[129] Furthermore, this change allows for the creation of a more se-

---

enacting legislation to promote the development of a PKE is that using public key cryptography and verifiable certificates is the best method for sending secure, authenticated messages over the Internet. *Id.* Therefore, legislation is needed to support these methods of transmitting secure transactions. *Id*

126. "Alternative procedures or requirements for the use or acceptance electronic signatures to establish the legal enforceability of contracts may accord greater legal status to the implementation or application of a specific technology or technical specification for performing the functions of creating electronic signatures." *See* Appendix 1.

127. Under the new section a "qualified security procedure" is one that is:

(1) previously agreed to by the parties; or
(2) certified by the Secretary of Commerce as being capable of creating, in a trustworthy manner, an electronic signature that:
  (A) is unique to the signer within the context in which it is used;
  (B) can be used to objectively identify the person signing the electronic record;
  (C) was reliably created by such identified person, and that cannot be readily duplicated or compromised; and
  (D) is created, and is linked to the electronic record to which it relates, in a manner such that if the record or the signature is intentionally or unintentionally changed after signing the electronic signature is invalidated.

128. The relying party must also show that the qualified security procedure was (i) commercially reasonable under the circumstances; (ii) applied by the relying party in a trustworthy manner; and (iii) relied on in a reasonable manner and in good faith by the relying party.

129. To receive protection as a secure electronic signature under the Illinois Act, the signature must be protected by a qualified security procedure. 5 Ill. Comp. Stat §§ 175/10-105. There are two ways to determine a qualified security procedure. First, it is a procedure that is mutually agreed upon by the parties. *Id.* § 175/10-110. Second, the Illinois Secretary of State certifies that a procedure is capable of providing reliable evidence that the electronic signature has not been altered. *Id* Additionally, the Secretary of State can certify that the procedure is capable of creating, in a trustworthy manner, an electronic signature that: (i) is unique to the signer within the context it was used; (ii) can be used objectively to identify the person signing the electronic record; (iii) was reliably created by

cure digital signature technology that may be far less expensive and far more accessible.[130] One of the most important features of this provision is that it allows the parties to determine what qualifies as a security procedure, which has several advantages. First, this provision still respects the principles of contracting—that parties must come to a meeting of the minds over certain provisions during contract formation. Second, this provision allows parties to use methods that may be more inexpensive and readily available for them to use in electronic transactions. Finally, allowing parties to come to an agreement regarding what constitutes a qualified security procedure for an electronic signature may provide the parties another, more simple, means of enforcement—breach of contract.

Allowing a state to pass technology specific legislation gives rise to a few concerns. There is the concern that parties with an advantage in bargaining power may use such a provision to the disadvantage of consumers. This concern could be resolved by adding a provision that prohibits a party from conditioning electronic transactions upon the use of a particular method of affixing electronic signatures.[131] A clear line would

---

that person; and (iv) if the record or the signature is intentionally or unintentionally changed after signing, the electronic signature is invalidated. *Id.*; *see generally* Behn, *supra* n. 125, at 215 (listing the six factors that a court must consider when determining whether a procedure is commercially reasonable). Determining whether a procedure is a "qualified security procedure" is a two-step process. The first step requires a finding that the security procedure is a qualified procedure; the second step, assuming the procedure is found to be qualified, indicates whether the qualified procedure is secure.

130. One of the reoccurring themes in the legislative history is a concern regarding technology-specific legislation. Some may assume that Congress did not want to be seen as playing favorites for a particular technology. However, congressional testimony indicates that the concern among businesses is that technology specific statutes may become outdated faster than technology neutral provisions. *See* Skogen Testimony, *supra* n. 43, at ¶ 9. The fear is that the technology industry is rapidly changing and with that so does the technology affecting electronic signatures. Technology specific statutes cannot be amended or modified fast enough with keep pace with the changes in technology. *Id.* (arguing that technology neutrality will serve to guard against regulations that quickly become outdated and impede the development of e-commerce, both domestically and internationally). Consequently, technology-specific statutes will hinder businesses from using the most cutting edge technology, which will most likely be more efficient, cost-effective, and user-friendly. *See id.* This not only indicates the fundamental problem with technology-specific legislation but also reveals the need for flexibility in the law. The way to address the concern is to create a statute that provides the flexibility for businesses to use the recent technology while assessing the security potential of such technologies. If the digital signatures increase the ability to authenticate the party and to verify the integrity of the transmission, it should receive greater legal protection. Such a statute does not deprive businesses of legal protection when using newer technologies and provides an incentive for the continued development of more secure electronic signature technologies.

131. *See* Sargent Testimony, *supra* n. 41, at ¶ 21. Including technology specificity within the legal protection of a uniform law is a power that could likely be exercised against one part of the computer information industry on behalf of another segment, which

be drawn in that the statute would not require the use of these secure technologies, but would require the parties to come to an agreement if they chose to use a secure technology.[132] Another concern is if one party uses a secure technology while the other party does not. While it is important to acknowledge, it is not a significant concern.[133]

The suggested provisions of E-Sign would also go further than both the original version of E-Sign and UETA by encouraging the use of a specific technology by giving them a presumption.[134] Parties using a

---

gives rise to "unfortunate implications of anti-trust." *Id.* at ¶ 21. Ms. Sargent frets that the lack of standards for exercise of the power is likely to lead to misuse. *Id.* These new provisions result in a perilous foray into federal-state relations by creating a law that dictates to the states the process in making rules of law. *Id.* at ¶ 26. There is the distinct possibility that these provisions exceed the boundaries of Congress' express powers. *Id.* Essentially, E-Sign gives state legislators a choice. State legislators must either allow federal law to govern an area that has been solely the province of the state or create a state law following the provisions established by federal law. If the legislators choose federal law, the federal law mandates that they choose whether E-Sign or UETA applies. In the event legislators decide not to follow E-Sign but that UETA with some modifications is more consistent with state common law, the legislators are in a Catch-22. If they modify UETA to accommodate state common law and preferences, E-Sign applies. On the other hand, if state legislators adopt UETA without modification, they have a version of UETA that might not be exactly consistent with state common law and preferences.

132. Of course, the statute must be clear on when an agreement between the parties has taken place. In order to be consistent with the rest of E-Sign and UETA, the provision would allow for an agreement to use a secure technology to be communicated via conduct and surrounding circumstances. For, example, if Party A uses his private key to affix a digital signature and Party B uses the corresponding public key, this action on the part of Party B is tantamount to consenting to use this secure technology.

133. This is not a significant concern because for both parties to use digital-signature technology, both parties must have or, at least, have access to the particular method of encryption and decryption. If Party A uses his private key to affix a digital-signature, Party B must use the corresponding public key to open the message. At the point that Party B opens the message using the public key, an agreement to use secure technology can be implied. On the other hand, if Party B does not have the technology to use the public key, then the message cannot be opened, authenticated, or its contents verified; the same holds true for using the hashing function. In the House version of E-Sign, H.R. 1714, there was a provision that prohibited a state from creating legislation that required the use of a technology that is not specific and is not publicly available. H.R. 1714 § 102(b). This provision could easily be resurrected and incorporated into the new section of E-Sign, which would ensure that any secure technology would be available to all parties.

134. *See* U.E.T.A. § 9(a) cmt. 4. UETA recognizes that there may be a greater legal protection for using a digital signature, but the amount of legal protection depends on the agreement between the parties. *Id.* While UETA does not provide a rebuttable presumption, it is feasible that there may be a rebuttable presumption if the parties agreed to it. *Id.* Once a signature is attributable to a person UETA provides that the effect of the signature will be determined in light of the surrounding context and surrounding circumstances, including any agreement between the parties. *Id.* For example, Alden and Acme agree that transmissions signed with signature dynamics require the recipient to prove that the message has been altered. Under UETA, signature dynamics may receive greater legal effect in this contractual relationship.

particular technology to produce an electronic signature would have a rebuttable presumption in a civil matter.[135] It is well established that these acceptable or secure technologies authenticate the party attaching a digital signature to a transmission and can indicate tampering or alteration with the content of the transmission.[136] Moreover, the ability of a party to repudiate the terms is vastly diminished, at the very least in comparison to other methods of attaching an electronic signature. Therefore, placing the burden of proof on the person attempting to repudiate the terms merely acknowledges the technical difficulties of repudiating the terms contained in a secure transmission.[137]

Creating a rebuttable presumption encourages people to use these secure methods while at the same time allowing them to use other means if it suits them.[138] Also, the creation of a presumption promotes the continued development of easier, more efficient, more secure, and cheaper methods of assigning digital signatures because of the advantage in using a technology that increases the capability to authenticate the sender and to verify message integrity.[139]

The new section 7002(a)(2) also contains a provision directing the U.S. Department of Commerce to draft, review, and classify the attributes for secure technologies, which serves as an important first step toward insuring the legitimacy and efficacy of new technologies.[140] More importantly, the new provision establishes certain preconditions that must be met before there is any evaluation of whether a technology qual-

---

135. "In resolving a civil dispute involving a secure electronic signature, it shall be rebuttably presumed that the secure electronic signature is the signature of the person to whom it correlates." Appendix 1.

136. Gripman, *supra* n. 1, at 779.

137. NCCUSL, Aug. 15, 1997, draft of UETA §§ 301-303 <http://www.law.upenn.edu/bll/ulc/ulc_frame.htm> (accessed Mar. 15, 2001). In the earlier drafts of UETA, there was a provision allowing the creation of secure electronic signatures. Behn, *supra* n. 125, at 225 (citing Ben Beard, Reporter's Memorandum http://www.law.upenn.edu/bll/ulc/ulc_frame.htm (accessed Mar. 15, 2001)) <http://www.law.upenn.edu/bll/ulc/uecita/etam/1197.htm> (accessed Mar. 15, 2001). NCCUSL omitted this provision from the final version because they feared that the technology and the market lacked the sophistication to fully utilize any presumptions. *Id.*

138. Clinton, *supra* n. 39, at ¶ 7 (stating that one of the essential principles of E-Sign is that the law should "give individuals and organizations maximum freedom to form contracts as they see fit").

139. *See e.g.* Behn, *supra* n. 125, at 208-209. One of the industries that would be affected by the increased legal protection for digital-signature technology is the certification authorities. *Id.* While the article presents four arguments as to why public key infrastructure should not be legislated right now, the article does not address giving greater legal effect to digital signature legislation while protecting other forms of electronic signatures. *Id.* at 209.

140. *See* 15 U.S.C. § 7005(b) (requiring the Secretary of Commerce and the Federal Trade Commission after 12 months of the enactment of E-Sign to file a report with Congress evaluating the benefits to consumers).

ifies as a secure one.[141] These preconditions allow for the scientific and technology communities to review the particular technology. Additionally, disclosure and notice provisions will make other businesses and consumers aware of another method of generating an electronic signature.[142] Accordingly, electronic signature technology will continue to grow and the comfort of business and consumers will increase.[143] By protecting the nonsecure electronic signatures as well as the secure ones, the new provisions of E-Sign will avoid the dangerous rigidity found in the current provisions of E-Sign.[144]

---

141. The preconditions are that: (i) the security procedure is completely open and fully disclosed to the public and (ii) the security procedure has been generally accepted in the applicable information-security or scientific community as being capable of functioning in a trustworthy manner.

142. Disclosure is essential because the Secretary of Commerce must determine whether the security procedure has been generally accepted in the applicable information-security or scientific community. Furthermore, the Secretary of Commerce must consider the opinion of independent experts in the applicable field and the published findings of such community, such as the American National Standards Institute, the International Standards Organization, the International Telecommunications Union, and the National Institute of Standards and Technology.

143. Behn, *supra* n. 125, at 217. "The concepts of a secure electronic record and a secure electronic signature, and the rebuttable presumptions that flow from that status, are critical to enabling a viable system of electronic commerce." *Id.* (citing 5 Ill. Comp. Stat. 175/10-120 cmt. (1)). Behn finds statements proclaiming that giving legal protection to digital signatures will increase e-commerce unfounded for two reasons. First, e-commerce appears viable without having to establishing rebuttable presumptions; second, e-commerce has grown at an explosive rate. *Id.* There are two problems with this reasoning. First, measuring explosive growth of e-commerce from the beginning of the e-commerce era is misleading because e-commerce began as early as four years ago. Measuring something that is as popular and widely used as the Internet from its inception is misleading. Second, by providing another reason for using digital signatures, business and consumers are more likely to use secure electronic signatures. An example of where the rebuttable presumption may assist consumers and the marketplace is in the purchase of automobiles. Ford Motor Company's research shows that 57 percent of consumers in the market for a new vehicle within the next year prefer to research their automotive purchase online, and 44 percent of consumers who use the Internet or online services have visited financial sites. Skogen Testimony, *supra* n. 43, at 7. About one-third of customers want to at least start the financing process online, according to Ford Credit research. *Id.* It goes without saying the consumers and automobile vendors may be more willing to begin these financial transactions if these presumptions were in place. "Uniform standards for electronic signatures would enhance public confidence in online applications of electronic commerce like [electronic funds transfer]." *Id.* at ¶ 8.

144. Sargent Testimony, *supra* n. 41, at ¶ 30. A serious impact is the inability of state law to react to technological change by not allowing the needed flexibility to respond to the eminent technological change. *Id.* Also, Behn argues that the rebuttable presumption does little to increase the international commerce. Behn, *supra* n. 125, at 217. This is unfounded given that the European Union ("EU") is considering a digital-signature directive that does precisely what these new provisions propose to do in that the EU would provide greater legal protection for electronic signatures produced by a certain technology. Pincus

CONCLUSION

E-Sign and UETA are legislative efforts to bring order and uniformity where there was a complete lack of organization and cohesion. The preemption provisions are inconsistent with the stated goals of creating legal uniformity and allowing e-commerce to realize its full potential.[145] The only way in which section 7002(a)(1) can foster uniformity is if E-Sign completely preempts the state version of UETA regardless of the degree of modification. The problem is that E-Sign does not make it clear that making minor modifications to UETA will lead to preemption of the state version. This lack of clarity leads to confusion and a lack of uniformity, which impacts the growth of e-commerce.[146] UETA and E-Sign were drafted because businesses and consumers were baffled by the lack of clarity and uniformity of the state laws. Ironically, the inability to define the relationship between E-Sign and UETA with specificity still creates an environment of legal uncertainty and a potential lack of uniformity.[147]

Section 7002(a)(2) while not erecting a barrier to uniformity or actively diminishing the growth of e-commerce is antithetical to the very foundation of any electronic signature statute. Authenticating the person signing a transmission and verifying the contents of a transmission are foundational principles of any signature provision. Currently, E-Sign mandates that all technologies be treated equally in that no specific technology will receive greater legal protection. This technology neutral approach is not the best way to promote e-commerce. A better way for E-Sign to promote e-commerce would be to give greater legal protection to specific technologies. Specific technologies encourage the use of those methods that are better able to authenticate and verify the integrity of a transmission.

Testimony, *supra* n. 52, at ¶ 12. Consequently, using the proposed method will make the uniform U.S. digital-signature law consistent with that of the EU's.

Technological methods of electronic attribution are evolving rapidly, and the creation of further authentication technologies will doubtlessly occur. *Id.* at ¶ 6. "The private sector today is using many forms of electronic authentication." *Id.* Most electronic transactions now occur in a closed system—systems where the parties with a preexisting relationship conduct electronic transactions under a mutually agreed system. *Id.* at ¶ 8. There is hope that in the distant future, there will be comprehensive, real-time authentication system. *Id.* Under the proposed provisions, a real-time method of authenticating an electronic signature falls within E-Sign even before verification that it is a secure method. This is evidence of the flexibility the new provisions provide. Additionally, the increased legal protection provides an incentive for businesses to work towards producing a real-time authentication system.

145. H.R. Rpt. 106-341(I), *supra* n. 42, Purpose and Summary at ¶ 1.

146. *See* Skogen Testimony, *supra* n. 43, at ¶ 10.

147. *See* H.R. Rpt. 106-341 (II), *supra* n. 43, Background and Need for the Legislation at ¶ 2.

These new preemption provisions are more forceful and less confusing than the current preemption provisions of E-Sign. The proposed section 7002(a)(1) clearly articulates the relationship between E-Sign and UETA to the point where there is no ambiguity. The proposed section 7002(a)(2) takes a very common sense approach in that it provides greater legal protection to those technologies that are able to authenticate the sender and to verify the integrity of a transmission. These proposed provisions provide clarity, uniformity, while promotion of secure technologies and the development of secure technologies. These goals are accomplished while respecting the role of UETA in creating clarity and uniformity.[148] These provisions create confidence in conducting business electronically and allow e-commerce to reach its full potential.

Renard Francois†

148. Sargent Testimony, *supra* n. 41, at ¶¶ 6-15. Two fundamental principles of UETA are to encourage and maximize the freedom of markets to achieve efficient and fair market solutions and to protect the freedom of both technology and markets to continue to evolve and develop. *Id.* at ¶ 17. Ms. Sargent notes another impact is on the federal court system. *Id.* at ¶ 31. Under the current preemption principles, it is possible that every contract case questioning the validity or legal effect of an electronic signature and record inherently contains a federal question. *Id.* Consequently, federal jurisdiction applies in a rather large number of cases in which federal jurisdiction presently is not now a question. While it is difficult to know for sure the impact on the federal courts, it is important to note the potential impact that this may have on the federal judiciary and their already crowded docket.

† The author is a staff attorney in the Bureau of Consumer Protection at the Federal Trade Commission in Washington, DC. The views expressed in this comment do not represent the position of the FTC. The author has obtained the following degrees: B.A., University of Pennsylvania; J.D., George Washington University Law School; LL.M. in Information Technology and Privacy Law, John Marshall Law School. The author would like to express his appreciation to Drs. Doris and Howard Francois, Ethel Wright, Leslie Reis, David Sorkin, Alex Wilson, Deborah McLochlin, Kristen Yoo, Frances Hadfield, and many others for their support and advice.

APPENDIX 1

PROPOSED NEW SECTION 15 U.S.C. § 7002

§ 7002. Exemption to preemption

(a) In general. A State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of section 7001 with respect to State law only if such statute, regulation, or rule of law—

(1) Any state statute, regulation, or other rule of law must constitute an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all 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) that is inconsistent with Titles I, Title II, or 7002(a)(2) the exception is preempted in its entirety.

(2)(A) specifies the alternative procedures, requirements, or alternative procedures or requirements part of any exception made under section 3(b)(4) of UETA 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 this title and title II [15 USCS § § 7001 et seq. and 15 USCS § 7021]; and

(ii) such alternative procedures or requirements may 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; if

(aa) through the use of a qualified security procedure, it can be verified that an electronic signature is the signature of a specific person, then such electronic signature shall be considered to be a secure electronic signature at the time of verification, if the relying party establishes that the qualified security procedure was:

(aa) commercially reasonable under the circumstances;

(bb) applied by the relying party in a trustworthy manner; and

(cc) relied on in a reasonable manner and in good faith by the relying party.

(B) a qualified security procedure for purposes of this Section is a security procedure for identifying a person that is:

(i) previously agreed to by the parties; or

(ii) certified by the Secretary of Commerce as being capable of creating, in a trustworthy manner, an electronic signature that:

(aa) is unique to the signer within the context in which it is used;

(bb) can be used to objectively identify the person signing the electronic record;

(cc) was reliably created by such identified person, and that cannot be readily duplicated or compromised; and

(dd) is created, and is linked to the electronic record to which it relates, in a manner such that if the record or the signature is intentionally or unintentionally changed after signing the electronic signature is invalidated.

(iii) a digital signature that is created using an asymmetric algorithm certified by the Secretary of Commerce shall be considered to be a qualified security procedure for purposes of identifying a person if:

(aa) the digital signature was created during the operational period of a valid certificate, was used within the scope of any other restrictions specified or incorporated by reference in the certificate, if any, and can be verified by reference to the public key listed in the certificate; and

(bb) the certificate is considered trustworthy because the certificate was issued by a certification authority in accordance with standards, procedures, and other requirements specified by the Secretary of Commerce, or the trier of fact independently finds that the certificate was issued in a trustworthy manner by a certification authority that properly authenticated the subscriber and the subscriber's public key, or otherwise finds that the material information set forth in the certificate is true.

(C) A security procedure may be certified by the Secretary of Commerce, as a qualified security procedure, following an appropriate investigation or review, if:

(i) the security procedure is completely open and fully disclosed to the public, and has been so for a sufficient length of time, so as to facilitate a comprehensive review and evaluation of its suitability for the intended purpose by the applicable information security or scientific community;

(ii) the security procedure has been generally accepted in the applicable information security or scientific community as being capable of satisfying the requirements of Section 7002(a)(2)(B)(ii) in a trustworthy manner; and

(iii) in making a determination regarding whether the security procedure has been generally accepted in the applicable information security

or scientific community, the Secretary of Commerce shall consider the opinion of independent experts in the applicable field and the published findings of such community, including applicable standards organizations.

PROPOSED NEW SECTION 15 U.S.C. § 7002(B)

(1)(a) In resolving a civil dispute involving a secure electronic signature, it shall be rebuttably presumed that the secure electronic signature is the signature of the person to whom it correlates.

(b) The effect of presumptions provided in this Section is to place on the party challenging the genuineness of a secure electronic signature both the burden of going forward with evidence to rebut the presumption and the burden of persuading the trier of fact that the nonexistence of the presumed fact is more probable than its existence.