ARTICLE

E-SIGNATURES—BASICS OF THE U.S. STRUCTURE

Holly K. Towle

TABLE OF CONTENTS

I. E-SIGNATURES: WHAT ARE THEY UNDER U.S. LAW?

A. Traditional State Law Regarding Signatures

For over fifty years, the most common definition of "signature" in the United States has been the definition of "signed" in section 1-201(39) of the Uniform Commercial Code (U.C.C.), a statute adopted by all U.S. states and containing basic definitions and principles for U.S. contracts. Article 1 defines

"signed" as including, "any symbol executed or adopted by a party with present intention to authenticate a writing."[1]

The U.C.C. is being updated in the United States. As each article is revised, the word "authenticate" is, or was,[2] being substituted for "sign."[3] "Authenticate" is the new term for "signature" adopted by the National Conference of Commissioners on Uniform State Laws (NCCUSL), a non-legislative body that drafts and supplies uniform or model legislation to U.S. state legislatures.[4] The new term "authenticate" includes *both* traditional and electronic signatures.[5] The definition varies slightly between NCCUSL statutes depending upon the statute's purpose and date of adoption.[6] The most meaningful definition under contract law is found in the Uniform Computer Information Transactions Act (UCITA), a new uniform act for computer information

1. U.C.C. § 1-201(39) (2000).

2. "Authenticate" is the term used in Revised Article 9 which has been adopted in fifty states; it was also the term used in proposed revisions to Articles 2 and 2A of the U.C.C. throughout the decade-long effort to revise them, and the term used in The Uniform Computer Information Transactions Act (UCITA), a NCCUSL uniform act approved in 1999. Without explanation, the 2001 draft of proposed revisions to U.C.C. Article 2 submitted to the NCCUSL's annual meeting (*see* U.C.C. § 2-103(o) (August 10–17, 2001 Draft)) used the word "sign" instead of "authentication," so it may be that the NCCUSL has changed course. If so, how it will deal with amendment of Revised Article 9 in fifty states is not known. It may also be that it has not changed course: an amended definition of "authentication" instead of "signed" was also made available at the 2001 annual meeting (copy on file with the author).

3. *See, e.g.*, U.C.C. § 9-102(a)(7) (2000); U.C.C. § 1-201(b)(3a) (Proposed Final Draft 2001); U.C.C. § 2-103(1)(a) (Tentative Draft, May 2001). Because of the different times and drafting committees for each definition, each has its own problems. Refer to note 34 *infra* and Part V.E *infra* (explaining that the revised Article 9 definition alters the traditional definition of "sign"). The purported basic purpose of each definition, however, is the same—to fashion a new definition of "signature" that will encompass both traditional and electronic signatures and also preserve all meanings of "signed" or "signature" as to each category.

4. *See* http://www.nccusl.org/nccusl/aboutus.asp. NCCUSL is an organization devoted to the promotion of uniformity in state law on all subjects where uniformity is desirable and practicable. To accomplish the NCCUSL's goals, its commissioners participate in drafting acts and endeavor to secure the acts' consideration by state legislatures. NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, REFERENCE BOOK 3 (1995–96). The NCCUSL is composed of approximately four commissioners from each state, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. *Id.* Commissioners are appointed by state governors and tend to be law school professors, legislators, practicing lawyers, and state code revisers. *Id.*

5. Refer to text accompanying note 8 *infra* (providing the UCITA definition of "authenticate"). *See also* UCITA § 102 cmt. 4 (commenting that "authenticate" is not limited to authenticating a writing), *available at* http://www.law.upenn.edu/bll/ulc/ucita/cita10st.htm.

6. For an example of a definition that should not be used outside its context, refer to note 34 *infra* and Part V.E *infra* (providing the definition used in U.C.C. Article 9).

transactions that has been adopted in Virginia and Maryland.[7] A word other than "signature" or "electronic signature" was chosen to emphasize that the signature need not be a traditional signature, that is, pen and ink on paper. In UCITA, "authenticate" means:

> (A) to sign; or
>
> (B) with the intent to sign a record, otherwise to execute or adopt an electronic symbol, sound, message, or process referring to, attached to, included in, or logically associated or linked with, that record.[8]

The word "record" makes it clear that the item signed need not be a piece of paper. In all of the NCCUSL statutes and in the federal Electronic Signatures in Global and National Commerce Act (E-Sign), "record" means: "[I]nformation that is inscribed on a tangible medium, or that is stored in an electronic or other medium and is retrievable in perceivable form."[9] Thus, information in an oral conversation is not in a "record," although it would be if the conversation were taped.

Why was the word "authentication" originally chosen by the NCCUSL to replace "signature"? The answer is historical, but hard to pinpoint. As explained by one source:

> The word "signature" has generally come to mean the name of a person written by the person or the person's autograph.
>
> . . . .
>
> [T]he purpose of a signature is to authenticate the writing to which it is affixed. A signature may also serve to give notice of its source, as well as *for the purpose and with the*

7. UCITA was adopted by the NCCUSL at its annual meeting in July, 1999. Examples of other uniform acts written by NCCUSL include the Uniform Trade Secrets Act and the Uniform Limited Partnership Act. *See* http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-utsa.asp; http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ulpa.asp. The Reporter for UCITA was Dean Raymond T. Nimmer, Leonard Childs Professor of Law at the University of Houston Law Center. UCITA is the product of submitted comments and numerous meetings regarding numerous drafts. Commentators included, but were not limited to: the NCCUSL Drafting Committee for UCITA; representatives of the American Law Institute; representatives of the software, publishing, banking, entertainment, information, and online industries; business and consumer end-users; federal regulators; various state bar associations; and several American Bar Association committees. *See* http://www.nccusl.org/nccusl/uniformact_attendance/uniformacts-attend-ucita.asp.

8. UCITA § 102(a)(6) (2000).

9. *See* U.C.C. § 5-102(a)(14) (2000); *id.* § 9-102(a)(69); *id.* § 1-201(b)(33a) (Proposed Final Draft 2001); *id.* § 2-103(1)(o) (Tentative Draft 2001); UCITA § 102(a)(55); Uniform Electronics Transactions Act (UETA) § 2(13) (1999); Electronic Signatures in Global and National Commerce Act (E-Sign), 15 U.S.C. § 7006(9) (2000) (defining "record" as information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form).

> *intent that the individual signing the writing shall be bound thereby*.[10]

The comments to the U.C.C. state:

> The inclusion of authentication in the definition of "signed" is to make clear that as the term is used in this Act [U.C.C.] a complete signature is not necessary. Authentication may be printed, stamped or written; it may be by initials or by thumbprint. It may be on any part of the document and in appropriate cases may be found in a billhead or letterhead. No catalog of possible authentications can be complete and the court must use common sense and commercial experience in passing upon these matters. The question always is whether the symbol was executed or adopted by the party with present intention to authenticate the writing.[11]

As noted in the Article 1 comment, the critical question is always whether the symbol adopted as a signature was executed or adopted by the party with the present intention to authenticate the writing. In *Parma Tile Mosaic & Marble Co. v. Estate of Short*[12] the question was whether the printed heading—showing the name of the sender on the top of a facsimile—constituted a signature for purposes of allowing the facsimile to serve as a signed guaranty.[13] The answer was "no" because, even though letterhead can count as a signature, it was not clear that the faxed heading had been supplied with the intent to sign the document—all fax machines print a heading showing the sender's name, but not all facsimiles are signed documents.[14] As in Article 1 and under the common law, the critical question in U.S. signature law is intent.

A study of Dutch legislation identifies these functions of signatures, all of which accord with U.S. traditions, that also include variations of the following:

---

10. 80 C.J.S. *Signatures* §§ 1, 3 (2000) (citations omitted) (emphasis added).

11. U.C.C. § 1-201 cmt. 39 (2000); *accord* Spevack, Cameron & Boyd v. Nat'l Cmty. Bank of New Jersey, 677 A.2d 1168, 1169 (N.J. Super. Ct. App. Div. 1996) (noting that a "signature" used to endorse a check may take many forms and need not be a signed name, and holding that the entry of a deposit account number on the back of a check was a sufficient signature because, "[i]n keeping with the electronic age, it is the numbers which have the primary significance").

12. 663 N.E.2d 633 (N.Y. 1996).

13. *Id.* at 633–34.

14. *Id.* at 634–35. *See also* Zemco Mfg., Inc. v. Navistar Int'l Transp. Corp., 186 F.3d 815, 821–22 (7th Cir. 1999) (noting that typed initials can suffice as a signature but, where the question was whether computer printouts containing the stamped or typed name "Navistar" were "signed," an issue of fact existed whether those markings were executed with the intention of authenticating the printouts).

> *Identification*. The addressee can verify the signer's identity by checking the signature.
>
> *Authentication*. The signature authenticates the declaration, which is included in the writing concerned. The writing reflects the facts correctly, unless evidence to the contrary is produced.
>
> *Declaration of will*. By signing the signer manifest his will and declares to be legally bound to the intention included in the writing concerned.
>
> *Authorisation*. The signer implicitly declares being authorized to perform a legal act, e.g., in case of representation.
>
> *Safeguard against undue haste*. By putting one's signature to a document the signer is notified that legal consequences may be involved. Thus, the signer is protected against undue haste.
>
> *Non-repudiation of origin and/or receipt*. The signer cannot deny that he has sent or received a document, unless proven otherwise.
>
> *Notice of contents*. The signer implicitly indicates that he knows the contents of the document.
>
> *Integrity*. Putting one's signature at the end of the document guarantees to some extent that the document has not been altered afterwards, thus, reducing the possibility of fraudulent actions.
>
> *Originality*. Signing a document enables to distinguish the original from a copy.[15]

An authentication or signature can be used for any or all of these and perhaps additional purposes. A use for fewer than all of these purposes is also perfectly appropriate depending upon the intention of the signing party.

For example, the person who signs the last page of a contract does so to adopt all of its terms (a "declaration of will"); when the same person initials each page, it is not to adopt the terms on that page (that has already been done by signing the last page), but to authenticate that, as of signing, the initialed page is the page that was in the document ("integrity" function, but per page, or "authentication" function). If the person uses a manual

15. *See* B.P. AALBERTS & S. VAN DER HOF, DIGITAL SIGNATURE BLINDNESS, ANALYSIS OF LEGISLATIVE APPROACHES TOWARD ELECTRONIC AUTHENTICATION § 4.3.1.1 (Nov. 1999).

signature or chop, each serves as a means to identify the person ("identification" function), but if the person signs with an X (for example, because he cannot manage a full signature), the X will be his signature ("declaration of will" function), but will not identify him. In all cases, the meaning of the signature or symbol depends on the *intention* of the acting party. If the X is adopted as a symbol of the party's signature, then that party has signed the contract. If the X is added to mark where the signature should be placed, when and if the contract is ever signed, then the X merely acts as a place-marker that is not a signature.

The definition of "authenticate" in UCITA is the most understandable and historically accurate definition for legal practitioners among the various NCCUSL statutes. UCITA preserves all meanings of "sign" by stating that "authenticate" means "to sign."[16] This picks up every possible meaning of "sign" (whatever these meanings may be), including electronic signatures, as it is not limited to any medium.[17]

The problem, of course, is that some laws requiring a "signature" might be construed as contemplating non-electronic signatures only, and thus subsection A of the UCITA definition would not be useful in those circumstances. Accordingly, subsection B addresses this problem by expressly stating that "authenticate" includes *electronic* signatures, that is, if subsection A is not enough, then any other means used to sign also counts, including electronic signatures such as "to execute or adopt an electronic symbol, sound, message, or process referring to, attached to, included in, or logically associated or linked with, that record."[18] Other formulations of these same concepts are possible, and the NCCUSL continues to work on a uniform definition that will reflect the other formulations in all of the NCCUSL statutes.[19]

16. UCITA § 102(a)(6)(A) (2000). Refer to text accompanying note 8 *supra* (quoting this section of UCITA).

17. *See* UCITA § 102 cmt. 4 (noting that the term "authenticate" is "technologically neutral").

18. *Id*. § 102(a)(6)(B).

19. Currently, the definition of "authenticate" in U.C.C. Article 9 creates unnecessary problems. Refer to note 34 *infra* and Part V.E *infra*. The definition of "sign" proposed in the August 10–17, 2001, draft of proposed U.C.C. Article 2-103(o) was also problematic and was amended at the 2001 Annual Meeting of NCCUSL. The amended definition, as of the meeting, returned to the term "authenticate" instead of "sign" (*see* note 2, *supra*) and defined it as follows: "(3a) '[a]uthenticate,' except as otherwise provided in _____, means (A) to sign; or (B) with the present intent to adopt or accept a record, to attach or logically associate an electronic symbol, sound, or process to or with the record." This new definition contains many of the same problems as the Article 9 definition (*see* note 34 *infra*) because it limits the functionality of signatures contemplated by subsection (3a)(B) to that of adopting or accepting a record (one function) when there

It is important to note that "authentication" as used in UCITA and the U.C.C. is *different* from the way "authentication" tends to be used in "digital signature" statutes dealing with public and private key encryption technology such as can be found in some U.S. states—Washington and Utah, for example.[20]

---

are many more functions that are critical to Article 2, the U.C.C., and contract law generally. Refer to the Dutch study in text accompanying note 15 *supra*. This proposed definition also repeats the Article 9 error of omitting elements of the E-Sign, UCITA, and UETA definitions which were designed to robustly enable e-commerce. Refer to note 34 *infra*. Last, this language changes signature law, presumably unintentionally. Under existing Article 1, the *symbol* must be executed or adopted with the present intent to *sign* (authenticate) a writing, an act (signing) that can cover at least eight functions. Refer to the study in text accompanying note 15 *supra*. Under the proposed U.C.C. Article 2 definition, the present intention is to adopt or accept the record, *not* the symbol. Not only does this change what is supposed to be adopted but, again, it limits the functions of a signature to just one function (adopting or accepting a record). There are many more functions, and none should be eliminated.

20. Such statutes apply only when a certain encryption technology is used, i.e., asymmetric cryptography. *See, e.g.*, WASH. REV. CODE § 19.34 (1998); UTAH CODE ANN. § 46-4-101 to 46-4-501 (2000). There are two basic types of encryption that illustrate the technology involved in coding a message for security. *See generally* BENJAMIN WRIGHT, THE LAW OF EDI, E-MAIL AND INTERNET: TECHNOLOGY, PROOF, AND LIABILITY §§ 1.3.1–1.3.2 (2d ed. 1997). First, the Data Encryption Standard (DES) establishes a standard mathematical algorithm for encoding and decoding messages. *Id.* § 1.3.1. The sender uses a "key" (a series of numbers) to scramble the message with the DES algorithm, and the recipient uses the same key to unscramble the message. *Id.* DES encryption is commonly used in electronic funds transfers. DES requires that the key be closely guarded, because anyone with the key can use the widely-known DES algorithm to decode messages made with the same key.

A second encryption system is known as public key encryption. *Id.* § 1.3.2. This is the kind of encryption upon which "digital signature" statutes such as Washington's Electronic Authentication Act are based. *See* WASH. REV. CODE § 19.34.020(11). Here again the algorithm must be known by both sender and recipient. WRIGHT, *supra*, § 1.3.2. (RSA is a patented public key algorithm licensed widely.) *See id.* Each person using the public key encryption system has two keys—a public key and a private key. *Id.* The public key decodes a message encoded with the same person's private key, and vice versa. *Id.* If each person keeps the private key confidential, he or she can distribute the public key widely to others who can then read the person's messages encoded with the private key. *Id.* Anyone who is able to decode a message with the public key can be certain that only the owner of the private key could have sent it. *Id.* Also, someone with the public key can send a secure message to the owner of the private key, because only the private key will decode the message. *Id.*

Further, after creating a message, the *sender* encrypts it with her private key and runs it through a "hashing algorithm." A "hashing algorithm" is a one-way algorithm that produces a resulting hash, or "message digest," if even one character of the message is changed after signing. Thus, if there is a change, the message hash received will not be the same as the sender's hash and the recipient will know that the message received is not the same as the message sent. The *recipient* runs the message through the same hash (used by the sender), creating his own message digest, and unencrypts the sender's message digest using the sender's public key. If the message digest sent matches the message digest created by the recipient, the recipient knows that only the sender could have sent the message (unless she lost control of her private key) and that the message did not change during transmission.

While the foregoing process is referenced as a "digital signature," there are many different approaches to digital signatures "such as fail-stop digital signatures, blind

In those statutes, and in many other instances, "authentication" is used to mean the process of determining whether someone or something is, in fact, who or what he or she declares to be—in other words, that he or she is authentic. Such usage focuses on the integrity of the record or on the attribution of a record or signature to someone, instead of focusing on whether the record is *signed*. In UCITA and the U.C.C., "authentication" focuses on whether the record is signed.

B. The Federal Electronic Signatures in Global and National Commerce Act—The Basic Thrust

On October 1, 2000, E-Sign became effective in the United States.[21] E-Sign only deals with electronic signatures, not all signatures, and establishes an equivalency between electronic and non-electronic records and signatures for transactions within E-Sign's scope.[22]

That scope pertains to "transactions"—a defined term including more than just contracts.[23] The part of E-Sign that establishes equivalency is only relevant "with respect to any transaction in or affecting interstate or foreign commerce."[24] There have been shifting trends regarding what constitutes "interstate commerce." However, in the context of computer crime, a federal district court recently determined that, since the advent of connecting computers to the Internet, almost all

signatures and undeniable digital signatures," the first of which allows a person to sign a document without knowledge of its contents. *See* AALBERTS & VAN DER HOF, *supra* note 15, § 1.2. These commentators also note that digital signatures are used for more than signing a document; they are also used to authenticate (as in "verify") the identity of something such as Web sites, computer software, servers and the like. *Id.* Such uses would be a version of the *"integrity"* purpose of a signature that is referenced in the textual example of traditional uses of signatures (e.g., initialing a page not to "sign" it, but to indicate that it really is a legitimate page of a document). Refer to text accompanying notes 15–18 *supra*.

21. E-Sign § 101, 15 U.S.C. § 7001 (2000).

22. *Id*. § 101(a)(1), 15 U.S.C. § 7001(a)(1).

23. E-Sign defines "transaction" as:

> . . . an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct—
>
> (A) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) services, and (iii) any combination thereof; and
>
> (B) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.

Id. § 106, 15 U.S.C. § 7006.

24. *Id*. § 101(a), 15 U.S.C. § 7001(a).

computer use has become "interstate" in nature.[25] E-Sign also contains express exceptions from its coverage.[26]

If a transaction is within E-Sign, the equivalency it creates is stated as follows:

> (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
>
> (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.[27]

The genesis in the United States of this "equivalency" rule is UCITA,[28] and it is there explained as follows:

---

25. Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc. 119 F. Supp. 2d 1121 (W.D. Wash. 2000). The claim in the case was brought under the Computer Fraud and Abuse Act which applies, in part, to "protected computers," defined as computers used in "interstate or foreign commerce" or communication.) *See generally id*.

26. E-Sign § 103, 15 U.S.C. § 7003. This section of E-Sign provides, in part, as follows:

> (a) Excepted Requirements.—The provisions of section 101 shall not apply to a contract or other record to the extent it is governed by—
>
> (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 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—
>
> (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.

Id. § 103(a)–(b), 15 U.S.C. § 7003(a)–(b).

27. *Id*. § 101(a), 15 U.S.C. § 7001(a).

28. UCITA provides that "[a] record or authentication may not be denied legal effect or enforceability solely because it is in electronic form." UCITA § 107(a) (2000). This wording, except for replacement of "authentication" with "signature," was repeated in section 7 of UETA and thus was picked up when E-Sign used portions of UETA.

> Equivalence of Electronics. Under subsection (a), the fact that a message, record or authentication is electronic does not alter its legal impact. This establishes an equivalence between electronic and other records. The rule refers to the form of the authentication or record, not to its content.[29]

The focus in E-Sign (and UCITA and UETA) is on the form of the record or authentication, that is, electronic versus non-electronic, and equivalency is established as to form. *Other* relevant issues are not disturbed. For example, if an electronic contract is signed by a minor who cannot legally make a contract, then the contract may be invalid under traditional contracting principles. But any invalidity must come from those principles—it cannot come solely from the fact that the contract was signed electronically or is evidenced by an electronic record.

So electronic signatures work, but what are they? E-Sign defines an electronic signature as follows:

> ELECTRONIC SIGNATURE.—The term "electronic signature" means 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.[30]

An electronic signature is merely one kind of an "authentication" under state law. If "authentication" were a circle, "electronic signatures" would fit inside the larger circle of "authentication." This is because an authentication includes *all* signatures, whether written, painted, stamped, or electronic, whereas the federal term "electronic signature" only deals with the electronic subset of the larger world of "authentication." As to the intersection of these worlds, the federal definition is the same as the definition in UETA, an act that deals only with the smaller subject of electronic signatures and not the larger circle of "authentications."[31] In contrast, UCITA and the U.C.C. deal with the larger circle so they use the broader term "authentication."[32] But the description of electronic authentications, at least in UCITA, is consistent or essentially identical to the E-Sign definition.[33] That is not the case with the U.C.C. Revised Article

29. *Id*. § 107(a) cmt. 2.

30. E-Sign § 106(5), 15 U.S.C. § 7006(5).

31. *See* UETA § 2 cmt. 7 (1999).

32. *See* UCITA § 102(a)(6); U.C.C. § 1-201(b)(3a) (proposed final draft 2001); U.C.C. § 2-103(1)(a) (tentative draft, May 2001).

33. *Compare* UCITA § 102(a)(6)(B), *with* E-Sign § 106(7), 15 U.S.C. § 7006(5).

9 definition, but preemption should not be an issue because E-Sign does not apply to U.C.C. Article 9.[34]

It is important to note that E-Sign does not require anyone to deal electronically. The statute expressly states that E-Sign does not require any person, other than certain governmental agencies, to agree to use or accept electronic records or electronic signatures.[35] Any such requirement, or lack of one, is up to the participants in any transaction covered by E-Sign. A primary sponsor of E-Sign provides this explanation:

> Section 101(a) establishes a basic federal rule of non-discrimination with respect to the use of electronic signatures and electronic records, including electronic contracts. Subject to the Act's consumer consent requirement (§ 101(c)) and specific exceptions (§ 103), this federal rule of non-discrimination means that a State generally cannot refuse to allow parties to use electronic signatures and electronic records in lieu of paper records and handwritten signatures. *This federal rule also means that if two parties agree with one another, electronically or otherwise, on the terms and conditions on which they will accept and use electronic signatures and electronic records in their dealings with one another and the parties could have entered into a comparable agreement regarding the use of signatures and records in the paper world, the State cannot refuse to give effect to the parties' agreement*.[36]

34. U.C.C. Revised Article 9 defines "authenticate" as "(A) to sign; or (B) to execute or otherwise adopt a symbol, or encrypt or similarly process a record in whole or in part, with the present intent of the authenticating person to identify the person and adopt or accept a record." U.C.C. § 9-102(7). This definition does not include all of the elements that are in the E-Sign, UCITA, and UETA definitions, which more robustly enable electronic commerce, for example, references to "electronic sounds," verbiage contemplating incorporated or associated terms, and language reflecting European terminology ("logically associated with"). UCITA § 102(a)(6)(B); UETA § 2(8). The Article 9 definition also creates a problem by making the "identification" function of some signatures a requirement for all signatures. That is not consistent with traditional signature law and would not appear to be consistent with E-Sign. Refer to Part V.E *infra* (identifying further problems with the article and definition). While the Article 9 definition may create unintended problems, it should not create a pre-emption issue because E-Sign excludes the entire U.C.C., except for portions of Articles 1, 2, and 2A. E-Sign § 103(a)(3), 15 U.S.C. § 7003 (a)(3).

35. E-Sign § 101(b)(2), 15 U.S.C. § 7001(b)(2).

36. 146 CONG. REC. S5283 (daily ed. June 16, 2000) (statement of Sen. Abraham) (emphasis added) [hereinafter Abraham Statement of June 16, 2000].

C. Interaction of E-Sign with the Uniform Electronic Transactions Act: Repeal of UETA is Advisable

UETA is a NCCUSL model act.[37] UETA was to be a procedural act that could be uniformly adopted by states for the purpose of enabling electronic commerce.[38] Many states have electronic "signature" statutes of one type or another,[39] but there is no uniformity. Thus, the NCCUSL appropriately decided it would be helpful to produce a minimum baseline for electronic commerce.

"Minimum" is the key word because UETA was intended to supply procedural, not substantive, rules for electronic commerce, and its scope was intentionally limited.[40] For example, it does not apply to laws governing wills or trusts, nor to the U.C.C. or UCITA, except for a portion of U.C.C. Articles 1, 2, and 2A (E-Sign includes these and other exceptions).[41] It was intended to enable e-commerce by, among other things, replacing portions of numerous state statutes—requiring "writing" or "signatures"—with rules allowing the use of electronic records and electronic signatures.[42]

Good idea, but badly implemented by the adopting states. California was the first state to adopt UETA, and it made a complete mess of it. For example, in a "uniform" "enablement" statute, California added the following list of exclusions:

> (c) This title does not apply to any specific transaction described in Section 17511.5 of the Business and Professions Code, Section 56.11, 56.17, 798.14, 1133, or 1134 of, Sections 1350 to 1376, inclusive, of, Section 1689.6, 1689.7, or 1689.13 of, Chapter 2.5 (commencing with Section 1695) of Title 5 of Part 2 of Division 3 of, Section 1720, 1785.15, 1789.14, 1789.16, 1789.33, or 1793.23 of, Chapter 1 (commencing with Section 1801) of Title 2 of Part 4 of Division 3 of, Section 1861.24, 1862.5, 1917.712, 1917.713, 1950.5, 1950.6, 1983, 2924b, 2924c, 2924f, 2924i, 2924j, 2924.3, or 2937 of, Article 1.5 (commencing with Section 2945) of Chapter 2 of Title 14 of Part 4 of Division 3 of, Section 2954.5 or 2963 of, Chapter 2b (commencing with Section 2981) or 2d (commencing with Section 2985.7) of

37. UETA introductory cmt.

38. *Id*. prefatory note & cmts. A & B.

39. *See* McBride Baker & Cole, Laws Authorizing Signatures (providing a table of electronic signatures statutes), *at* http://www.mbc.com/ecommerce/legislative-_1.asp?state=all (last visited Aug. 22, 2001).

40. UETA prefatory note cmt. B.

41. *Id*. prefatory note cmt. A.

42. *Id*. prefatory note cmt. B.

> Title 14 of Part 4 of Division 3 of, or Section 3071.5 of, the Civil Code, subdivision (b) of Section 18608 or Section 22328 of the Financial Code, Section 1358.15, 1365, 1368.01, 1368.1, 1371, or 18035.5 of the Health and Safety Code, Section 658, 662, 663, 664, 666, 667.5, 673, 677, 678, 678.1, 786, 10083, 10086, 10087, 10102, 10113.7, 10127.7, 10127.9, 10127.10, 10197, 10199.44, 10199.46, 10235.16, 10235.40, 10509.4, 10509.7, 11624.09, or 11624.1 of the Insurance Code, Section 779.1, 10010.1, or 16482 of the Public Utilities Code, or Section 9975 or 11738 of the Vehicle Code. An electronic record may not be substituted for any notice that is required to be sent pursuant to Section 1162 of the Code of Civil Procedure. Nothing in this subdivision shall be construed to prohibit the recordation of any document with a county recorder by electronic means.[43]

One does not even need to look up each statute to see that it might be easier and more cost effective in California to use paper than to locate and review each listed statute and determine to what the California UETA does or does not apply. So much for interstate commerce. And it got worse because California added ill-advised, non-uniform amendments such as the following:

> Except for a *separate* and optional agreement the *primary purpose* of which is to authorize a transaction to be conducted by electronic means, *an agreement to conduct a transaction by electronic means may not be contained in a standard form contract that is not an electronic record*. An agreement in such a standard form contract may not be conditioned upon an agreement to conduct transactions by electronic means. An agreement to conduct a transaction by electronic means may not be inferred solely from the fact that a party has used electronic means to pay an account or register a purchase or warranty. *This subdivision may not be varied by agreement*.[44]

The rule could be interpreted as follows: if parties are covered by California's UETA but use a non-electronic standard form contract (this term is not defined), they may not include in that contract any agreement to conduct a transaction by electronic means. Accordingly, it appears that:

> ?? If a franchiser uses a paper standard form franchise agreement, no clause of the agreement may require the franchisee to order inventory or to provide global notices electronically because the primary purpose of the written agreement is to create a franchise relationship—

43. CAL. CIV. CODE § 1633.3(c) (West 1999).

44. *Id*. § 1633.5(b) (emphasis added).

not to authorize electronic transactions. That result may not be varied by agreement, even though commercial parties routinely make such contracts.

?? If a manufacturer uses a paper standard form distribution agreement, no clause of the agreement may require distributors to check a Web site for changes in pricing, packing, production standards, or anything else because the primary purpose of the written agreement is to create a distribution relationship—not to authorize electronic transactions. That result may not be varied by agreement, even though commercial parties routinely make such contracts.

?? If a broker uses a paper standard form account agreement that sets forth the terms for all transactions with that brokerage house, whether by "land line" telephone, cellular phone, postal mail, e-mail, Internet, or in-person visits. The clauses in the agreement governing electronic transactions must be moved out of that agreement and put into a *separate agreement*, because the primary purpose of the agreement might or might not be viewed as for electronic transactions. This result may not be varied by agreement between the broker and any commercial or consumer customer even though they routinely make such contracts and may want the multiple methods of access to brokerage services to be covered by one contract.

?? If a credit card issuer uses a paper standard form contract and states that, instead of providing written notice of a lost card, consumers may report the loss and avoid exposure if they use a specific telephone number, is the clause enforceable? Apparently not under California law, even though such a contract would decrease harm and risk and ease reporting burdens for consumers.

The perceived problem that the California amendment was apparently intended to solve, easily could have been solved other ways or was already solved by existing law.[45] Obviously, states—

45. Based on e-mail traffic, it appears the California legislature was attempting to address a situation in which, for example, a consumer physically goes to her bank and obtains a paper mortgage, the 15th clause of which provides that notice of foreclosure can be provided by e-mail. The concern was that the consumer might not even have a computer and thus could not receive electronic notice. *See* Holly Towle, *The Uniform Electronic Transactions Act–The California Amendments*, 4 CYBERSPACE LAW. No. 918 (1999). How else could that concern have been met without disrupting or freezing the development of legitimate commercial practices and efficiencies that benefit customers, including consumers?

or at least California—could not be trusted to deal judiciously with e-commerce or consider the needs of commerce beyond the state's borders, that is, interstate e-commerce. Enter the federal government. Seeing a train wreck coming if other states followed California's lead, E-Sign was born.

Fast forward to today. E-Sign is federal law and numerous states have enacted UETA.[46] Some states have not adopted UETA because close study reveals that it contains substantive problems that are best avoided, in general, and some problems that can only be avoided by not adopting UETA.[47] This latter

---

Section 8 of UETA is contained in the California statute, and that section already addressed this concern by preserving substantive provisions of other laws such as delivery requirements. UETA § 8; CAL. CIV. CODE § 1633.8. It is true UETA section 8 was partially rejected in E-Sign § 102(c). *See* E-Sign § 102(c), 15 U.S.C. § 7002(c) (2000). However, California did not know that when it amended UETA, and instead of correcting the UETA problem—as E-Sign did—California made it worse. As for laws other than UETA, traditional common law, U.C.C., and UCITA contracting concepts also deal with the perceived problem. For example, if a court viewed the 15th clause as substantively or procedurally unconscionable, it could invalidate it in most states. Unfair acts and practices would also be relevant in circumstances in which consumers might not even have computer access. In fact, the hypothesized notice might not even count as notice under typical contract law:

> It is also true that not everyone has access to electronic information but to the extent that these facts suggest that electronics should not suffice for writings in consumer cases, the argument contains an assumption that an e-mail message sent to a consumer who has no e-mail address would be treated as an adequate notice under a consumer protection laws (sic) requiring a written notice. That claim is at best disingenuous. A general rule of technological adequacy does not erase other requirements for effective notice or signature. A letter intentionally mailed to a physical address that is not the address of the intended recipient is unreasonable and ineffective. The same rule applies to electronics.

Raymond T. Nimmer, *Electronic Signatures and Records: The New US Perspective*, 17 No. 12 COMPUTER & INTERNET LAW. 8, 16 (2000) (examining state and federal legislation shaping the adequacy of electronics to fulfill writing or written signature requirements).

The U.C.C. requires that any notice entail sending the information in a manner reasonably calculated to be received. *Id.* at n.39 (citing U.C.C. § 1-201 (1998) and UCITA § 102(a)). UCITA follows the same rule.

E-Sign expressly dealt with this issue by avoiding coverage of certain sensitive transactions such as acceleration and foreclosure notices, by requiring affirmative consumer consent to receipt of electronic disclosures when written consumer disclosures are required by applicable law, and by including in the consumer consent rule a requirement that consent be provided electronically. *See* E-Sign § 101(c)(1)(A), 15 U.S.C. § 7001(c)(1)(A); § 101(c)(1)(C)(ii), 15 U.S.C. § 7001(c)(1)(C)(ii); § 103(b), 15 U.S.C. § 7003(b). This latter rule is a self-proving means of ensuring that the consumer has access to a computer or other device that allows receipt of electronic information.

46. Thirty-six states have enacted some form of UETA. *See* THE NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, A FEW FACTS ABOUT THE UNIFORM ELECTRONIC TRANSACTIONS ACT, *at* http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp (last visited July 30, 2001).

47. *See, e.g.*, UNIFORM ELECTRONIC TRANSACTIONS ACT REPORT OF LAW OF COMMERCE IN CYBERSPACE COMMITTEE (Business Law Section of the Wash. State Bar Assoc.), Nov. 6, 1999, § C [hereinafter UETA Report] (discussing some of the substantive

circumstance arises because UETA provisions frequently do not allow alteration by contract, even between commercial parties and even though the development of e-commerce is in its infancy.[48] As noted in the Dodd Report,[49] there are a few areas in which UETA would apply and E-Sign would not, and thus some argue that UETA still has utility. An example is intrastate transactions: where E-Sign would not apply and a state's UETA would. But again, any benefits of UETA coverage are not outweighed by the problems it creates,[50] particularly when several of those problems are avoided in E-Sign.

One might logically ask why this is even worth talking about given that E-Sign is federal law and UETA is state law. Cannot UETA, therefore, be completely ignored? No. E-Sign provides as follows:

> SEC. 102. EXEMPTION TO PREEMPTION
>
> (a) IN GENERAL.—A State statute, regulation, or other rule of law may modify, limit, or supersede *the provisions of section 101 with respect to* ***State*** *law only if such statute, regulation, or rule of law—*
>
> (1) *constitutes an enactment or adoption of the Uniform Electronic Transactions Act* ***as approved and recommended for enactment*** *in all the States by the National Conference of Commissioners on Uniform State Laws* ***in 1999*** . . . or
>
> (A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if—
>
> (i) such alternative procedures or requirements are consistent with this title and title II; and
>
> (ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the

problems with UETA), *at* http://www.wsba.org/sections/biz/lccc/report/1999.htm. *See also* Jeff Dodd, *Federal E-Sign and UETA: Proposed State Bar Report and Recommendation* [hereinafter Dodd Report] (recommending either adoption of E-Sign rules as Texas state law, that no further action be taken to modify Texas law, or that studies be undertaken to determine if particular aspects of state law might still benefit from electronic validation rules). Refer to Appendix 1 *infra*. Notwithstanding this report, it appears that UETA is, unfortunately, under consideration for adoption in Texas.

48. *See* UETA Report, *supra* note 47, § C(6)–(7) (noting problems with UETA's prohibition on varying specific sections by agreement of the commercial parties).

49. Refer to note 47 *supra* and Appendix 1 *infra*.

50. *See* Dodd Report, *supra* note 47, at Part V (comparing substantive differences between E-Sign and UETA and which would give Texas the best law for electronic adequacy).

> 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; and
>
> (B) if enacted or adopted after the date of the enactment of this Act, makes specific reference to this Act.[51]

This rule creates an impossible situation for anyone endeavoring to comply with applicable law. The following is the kind of analysis a practitioner or business must go through with respect to every state enacting UETA:

1. Could the law of the state apply to your contract?

2. If yes, has the state enacted UETA? If no, then comply with E-Sign and other state laws that are both consistent with E-Sign and that meet its other requirements—such as the requirement for technological neutrality. This requirement is set forth in section 102 (a)(2)(A)(ii).[52] UCITA is consistent, but other state laws may or may not be.

3. If yes, is the state's version of UETA identical to the version approved and recommended for enactment by the NCCUSL in 1999? Find the NCCUSL 1999 version and compare it word for word. Do this for each UETA state whose law might apply to the contract.

4. As of this writing, most (if not all) states have not enacted a version of UETA that is identical to the 1999 NCCUSL version.[53] Some variations are administrative, but many are substantive.

   A. If there is any variation, may UETA be completely ignored (that is, does E-Sign impose an "all or nothing" test regarding the "purity" of state UETAs)? If yes, start the E-Sign section 102 "consistency" analysis (Step 5).

   B. Some argue that UETA can never be completely ignored and that you must comply with the identical parts and ignore only the parts that vary from E-Sign.[54] Are those commentators correct, and if they

51. E-Sign § 102(a), 15 U.S.C. § 7002(a) (emphasis added).

52. Refer to note 51 *supra* and accompanying text (allowing states to supersede federal pre-emption provided that state law does not accord greater legal status to a specific technology or technologies).

53. *See* Dodd Report, *supra* note 47 (revealing that, as of that writing, no states had enacted UETA in its pure form, although many of the changes have not been substantive).

54. *See* Robert A. Wittie & Jane K. Winn, *Electronic Records and Signatures Under*

are, how will you know that they are, absent judicial decisions that will take years to emerge and that will vary among states?

C. Some argue that "immaterial" variations do not disqualify UETA from being identical to the 1999 NCCUSL version.[55] If that is correct, then determine which variations are material and which are immaterial, and then ignore the material variations. This might be possible for *truly* immaterial variations, such as section numbering, but there is a vast, graduating landscape between that kind of variation and the kind of variation found in section 1633.3(c) of the California UETA.[56] Do this analysis for each UETA state whose law might apply to the contract. For fun, once you get done, consider whether you would be willing to render a legal opinion on your conclusion!

5. If the state's UETA is not identical to the 1999 NCCUSL version, then does the state's version pass muster under E-Sign section 102(a)(2)(A)(i)?[57] That section saves state laws if they are "consistent" with Title I and Title II of E-Sign. As to each and every change in UETA made by each state, you must determine whether the change is consistent with Title I and Title II (good luck). Do this for each UETA state whose law might apply to the contract. To understand the difficulty of this, start with California's UETA.[58]

6. If the state's UETA passes the section 102(a)(2)(A)(i) test and is also technologically neutral, then how far have you really gotten? Not very, as you will now have to comply with potentially fifty versions of UETA that are different, but nevertheless consistent, with E-Sign as to state law.

7. What about federal law? You have to comply with E-Sign anyway as to federal law because a state may only

---

Federal E-Sign Legislation and the UETA, 56 BUS. LAW. 293, 329–30 & n.186 (2000) (noting that a key question of interpretation will be whether E-Sign's requirement for a pure UETA should be applied to the entirety of the non-conforming version of UETA or only to the non-conforming provisions). Ultimately, Wittie & Winn conclude that the appropriate reading of E-Sign is the "all or nothing approach," that is, the entire state version must be pure, not just particular provisions. *Id.* at 330–31.

55. *See id.* at n.185 ("Presumably non-substantive changes, such as formatting, section numbering and the like, would not be enough to cause a state's version of UETA not to be considered the 'official' version.").

56. Refer to note 43 *supra* and accompanying text.

57. Refer to note 51 *supra* and accompanying text (requiring that state laws modifying or superceding E-Sign demonstrate consistency with Titles I and II).

58. Refer to notes 43–44 *supra* and accompanying text (showing one of the non-uniform provisions of California's UETA).

supersede or vary E-Sign as to state laws.[59] Thus, any state efforts to supersede E-Sign by adopting UETA are simply not worth the candle. Even practitioners and businesses in a state with a "pure" UETA will have to deal with E-Sign in any case, so why create a double structure and an impossible and costly analysis for those attempting to comply with applicable law or attempting to engage efficiently in e-commerce?

For example, the Federal Truth in Lending Act (TLA) requires certain consumer disclosures to be made in writing,[60] and thus section 101(c) of E-Sign will apply to TLA disclosures.[61] Accordingly, you must comply with the complex provisions of E-Sign section 101(c) and with the Federal Reserve Board regulations that add requirements.[62] After you have done that, must you also comply with the consumer and other provisions of UETA in relevant states, even though E-Sign's subsection (c) was intended to address all (and more) of the concerns contemplated by UETA? Start the analysis described in Steps 1-7 above as to each UETA state. If you emerge with any sanity, and if you conclude that (1) the answer is yes, or (2) you haven't a clue as to the answer and thus will either ignore each state's UETA or comply with each of them, then—between UETA and E-Sign—e-commerce will have become so cumbersome that everyone would be better off to go back to pen and paper. But, the answer should be "no" in this example because E-Sign only allows UETA to alter E-Sign with respect to state law.

But what about states that have "state" truth-in-lending acts? These kinds of "state mirror" statutes start out paralleling a federal statute in order to provide jurisdiction

59. Refer to note 51 *supra* and accompanying text (indicating that state statutes or regulations may modify or supercede E-sign only in regards to state law).

60. *See, e.g.*, 12 C.F.R. § 226.17 (2000) (quoted in text surrounding note 133 *infra* and requiring closed-end credit disclosures to be in a writing and in a form the consumer may keep).

61. E-Sign § 101(c), 15 U.S.C. 7001(c) (2000) (allowing delivery of an electronic record in place of a statutorily mandated writing provided that the consumer consents and is provided with a notice of factors listed in E-Sign).

62. *See, e.g.*, 66 Fed. Reg. 17,341 (May 30, 2001). The Federal Register Bulletin's (FRB) interim rule regarding Regulation Z to implement Subsection (c) for the Truth in Lending Act. In the staff commentary to this interim rule, the staff states that "regardless of the technology used to meet this requirement, [E-Sign definition of electronic signature], the process must evidence the consumer's identity." Yet signature law, including E-Sign, does not require a signature to identify the signing party. But for the regulation itself, 12 C.F.R. § 226.36(f), which states that any e-signature satisfying E-Sign also satisfies the FRB regulation, the staff commentary would exceed the FRB's authority. Refer to Part V.E *infra* and 66 Fed. Reg. 17,329, 17,339 (May 3, 2001).

> to state regulators. Over time, the state statutes fall behind changes to the federal statutes and regulations, creating a Catch-22 in which compliance with a federal change may create a violation under the lagging state statute (states cannot adopt, in advance, changes in federal law because of issues concerning unconstitutional delegations of legislative authority). In such a circumstance, would you have to comply with UETA as to the state statute and with E-Sign as to the TLA? The only certain answer is that litigation will result and compliance will take a nose-dive as legal counsel, businesses, and consumers grapple with the scope and intersection of federal preemption, particularly with respect to consumer protection statutes such as the TLA versus the state mirror statute. The resulting costs to businesses and consumers can in no way be justified.

Is the above a correct analysis? No one knows, and that is the point. There are many interpretations of the interaction between E-Sign and UETA, and only litigation will determine which is correct. For example, is or is not section 1633.5(b) of the California UETA preempted such that the franchiser, manufacturer, broker, credit card issuer, or consumer described above may safely ignore it?[63] If you cannot definitely answer that question, you cannot deny there is a problem for everyone.

A way to avoid this chaos is to not enact UETA at all or, if a state has already enacted it, to repeal it. That will leave E-Sign standing alone as a uniform rule and all other (non-UETA) state laws must be consistent with E-Sign or are clearly preempted. Any gaps created can be handled by a more surgical approach designed to target the gap. For example, the Dodd Report (Appendix I) suggests several alternatives, such as enacting E-Sign as state law or undertaking to determine if particular aspects of state law may still benefit from electronic validation rules.[64] The report concludes, correctly, that either alternative is better than adopting or retaining UETA, stating:

> On this issue, I believe that the clear answer is that adoption of UETA would produce substantive less useful and effective rules than exist under current law or under a state enactment of federal standards. Stated simply, in

63. Refer to CAL. CIV. CODE § 1633.5(b) (West 1999). The California UETA contains non-uniform provisions that prevent ordinary contracting practices. Refer to note 44, *supra* and accompanying text.

64. Dodd Report, *supra* note 47, at Part II (arguing that both the status quo and enactment of E-Sign are superior alternatives to adopting any form of UETA).

> terms of promoting electronic commerce and protecting consumer interests, the Federal Act is better law.[65]

UETA's purpose has been well fulfilled by E-Sign, and the NCCUSL may justly, and commendably, take credit for the fact that E-Sign largely copies two NCCUSL products: UETA and UCITA. Does E-Sign itself have flaws and gaps? Yes, just like all legislation ever written. But E-Sign avoids many of the serious mistakes made in UETA.[66] Further, E-Sign creates uniformity and does not require answers that are impossible to determine, even at any cost.

II. SHOULD E-SIGNATURES BE CONFINED TO PARTICULAR TECHNOLOGIES?

In the United States, the answer to whether e-signatures should be confined to particular technologies is no longer the subject of debate. As a matter of federal law, the answer is "no." Section 101 of E-Sign establishes equivalency of electronic and non-electronic records and signatures and establishes certain other basic principles.[67] With respect to section 101, state laws that attempt to impose requirements for particular technologies are superseded:

> SEC. 102. EXEMPTION TO PREEMPTION
>
> (a) IN GENERAL.—A State statute, regulation, or other rule of law may modify, limit, or supersede *the provisions of section 101 with respect to State law only if such statute, regulation, or rule of law*—
>
> (1) constitutes an enactment or adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment in all the States by the National Conference of Commissioners on Uniform State Laws in 1999 . . . [no state as yet met this requirement] or
>
> (2)(A) *specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures* to establish the legal effect, validity, or enforceability of contracts or other records, *if*—
>
> (i) such alternative procedures or requirements are consistent with this title and title II; and

65. *Id.* at Part V.

66. Refer to Part V *infra* (discussing the mistakes being made in electronic commerce).

67. E-Sign § 101, 15 U.S.C. § 7001 (2000).

> (ii) *such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures*; and
>
> (B) if enacted or adopted after the date of the enactment of this Act, makes specific reference to this Act.[68]

There is a debate in the United States regarding the meaning of this section. Some argue that it eliminates all "digital signature"—public and private key encryption—state statutes. They argue that, by definition, such statutes attempt to alter the federal rule regarding technological neutrality by according specified benefits and burdens to signatures that utilize certain encryption.[69] That argument, however, ignores the fact that section 101 is very limited,[70] and that E-Sign only acts upon state laws that attempt to alter section 101 principles; for example, those state laws that attempt to say a signature cannot be electronic unless it is provided with a given technology. If the state law honors electronic signatures generally, no matter the

---

68. *Id.* § 102(a), 15 U.S.C. 7002(a) (emphasis added).

69. *See, e.g.*, Wittie & Winn, *supra* note 54, at 300, 333–36 (suggesting, apparently, that by assigning legal significance to the use of one particular technology, the Utah Digital Signature Act would not satisfy the technological neutrality standard of E-Sign). In fact, Wittie & Winn may only be suggesting that where a state mandates *only* one kind of e-signature and does not allow others, that such is pre-empted. *Id.* That would be consistent with the view stated in this paper *infra*.

70. One commentator explains the scope of section 101:

> The primary rules of the E-Sign Act for general contract law are in the following subsections of section 101.
>
> ?? Section 101(a): law may not deny legal validity to any signature, contract or other record "*solely* because it is in electronic form." Section 101(c) establishes consumer rules, but subsection (c) is a derogation from subsection (a), the primary rule.
>
> ?? Section 101(h): law cannot alter effect of contracts involving electronic agents.
>
> ?? Section 101(d): law requiring *retention* of a record or production of an original is met by certain electronic records.
>
> ?? Section 101(g): regulations are set forth regarding use of electronic signatures in notarization and the like.
>
> ?? Section 101(j): limitations are presented on the liability risk for insurance agents from use of electronic procedures.
>
> These mandatory rules define the preemptive scope of the E-Sign Act since they mandate outcomes notwithstanding that state law may provide a different result. Outside the scope of these rules, however, there is no basis in the stated policy of the E-Sign Act or in the statutory language to support a broader preemption of state substantive law or state signature law.

Nimmer, *supra* note 45, at 20 (footnotes omitted) (emphasis added).

technology, but also happens to provide certain benefits if particular technologies are used, such statutes should not be disturbed. This view, which would appear to be the better view, is expressed by Professor Raymond T. Nimmer in the following hypotheticals:

> *A state law provides that* electronic records and signatures will be *recognized only if they use a particular, designated technology*. This is a "mandatory digital signature law." Is that law preempted? Yes. By validating only one type of electronic record or signature and denying all other electronic records, it denies effect to the other electronics solely because they are electronic. Section 101(a) bans that. The result is that electronics using the designated technology and electronics using any other technology are enforceable under law as altered by the E-Sign Act.
>
> *A state law provides that*, if the parties opt to use a specific *technology, the results of using that technology 1) satisfy the signature and the writing requirement, and 2) create a presumption that the party identified by the technology was the party actually using it. This is an "optional* signature law" since it does not preclude use of other electronics or require parties to use one method. This approach describes most modern secure signature or digital signature statutes. Does the E-Sign Act preempt such statutes? No, but it does change part of the framework in which this law applies.
>
> The federal E-Sign Act does not deal with state law on when or whether a signature or record is attributed to a person and does not deal with state laws that determine whether obligations exist that are chargeable to a person. The E-Sign Act expressly excludes any change in the law on rights or obligations of persons under other law. That rule clearly preserves the second part of the hypothetical law previously stated. Even without that rule, attribution, obligation, and the like are not covered by the E-Sign Act. A statute does not preempt rules outside its coverage unless the E-Sign Act specifically so provides or purports to entirely dominate the entire field. The federal Act does not do so here. The only way to argue for a different result under the E-Sign Act would be to argue that the Act's rule which on its face merely bars state laws that invalidate electronic records actually contains an implied invalidation or policy that invalidates any state law that gives enhanced effect to certain technologies the E-Sign Act itself does not establish. This argument ignores preemption jurisprudence and the simple purpose of the E-Sign Act: to validate electronics. It attempts to read in preemptive coverage of a topic that the Act specifically does not address.

> The E-Sign Act, however, does supplant rules that deny enforcement of electronic records solely because they are electronic. In our "optional digital signature" illustration, the E-Sign Act converts any underlying state statute of frauds into a rule that requires a writing or an electronic record. This precludes any part of the hypothetical statute that implicitly gave effect only to signatures or records created with a particular technology. It renders the first statement in the hypothetical (which validates the electronics) irrelevant.
>
> The result: electronic and written records are equivalent, but procedures recognized in state law which give presumptions to users of particular procedures are not disturbed.[71]

While E-Sign should not invalidate optional digital signature statutes in the United States, the United States is serious about technological neutrality. How serious can be seen by looking at Title III of E-Sign.[72] Under that Title, the Secretary of Commerce is instructed to take all actions necessary to reduce impediments to the development of electronic commerce in foreign commerce, consistent with several principles.[73] Several of those principles stress the need and value of allowing parties to determine the issues relevant to electronic commerce by contract. One of those principles, as stated below, is that of technological neutrality:

> TITLE III—PROMOTION OF INTERNATIONAL ELECTRONIC COMMERCE
>
> SEC. 301. PRINCIPLES GOVERNING THE USE OF ELECTRONIC SIGNATURES IN INTERNATIONAL TRANSACTIONS.
>
> (a) PROMOTION OF ELECTRONIC SIGNATURES.— . . .
>
> (2) PRINCIPLES.—The principles specified in this paragraph are the following: . . .
>
> (B) *Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced*.

71. *Id.* at 20–21 (footnotes omitted).
72. E-Sign § 301, 15 U.S.C. § 7031.
73. *Id*.

> (C) *Permit parties to a transaction to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid.*
>
> (D) *Take a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions.*[74]

This approach signals a basic difference between the U.S. approach to e-signatures and some other approaches. The U.S. approach assumes that the parties will best know what kind and level of technology to use. Thus, legislation should permit parties to determine those technologies and allocate the risks of their use by agreements that should be honored in other jurisdictions—even if particular technologies are not used. Senator Abraham, one of the chief drafters of E-Sign, explains Title III as follows:

> Foreign nations may choose to adopt their own approach to the use and acceptance of electronic signatures and electronic records. In such cases, the Secretary should encourage those nations to provide legal recognition to contracts and transactions that may fall outside of the scope of the national law and encourage those nations to recognize the rights of parties to establish their own terms and conditions for the use and acceptance of electronic signatures and electronic records.
>
> *There is particular concern about international developments that seek to favor specific technologies of processes for generating electronic signatures and electronic records. Failure to recognize multiple technologies may create potential barriers to trade and stunt the development of new and innovative technologies.*
>
> *Unfortunately, international developments on recognizing electronic signatures are troubling. The German Digital Signature Law of July 1997 runs counter to many of the widely accepted principles of electronic signature law in the United States. For example, the German law provides legal recognition only to signatures generated using digital signature technology, establishes licensing for certificate authorities, and sets a substantial role for the government in establishing technical standards. Further, a position paper on international recognition of electronic signatures released by the German government (International Legal Recognition of Digital Signatures, August 28, 1998) seeks to apply these principles internationally. This policy statement reemphasizes the principle that uniform security standards*

74. *Id*. (emphasis added).

> *are necessary for all uses of digital signatures regardless of their use, supports mutual recognition of digital signatures only to those nations which have a similar regulatory structure for certification authority, and fails to provide legal effect to electronic signatures generated by other technologies.*
>
> The European Community is considering a framework for the use and acceptance of electronic signatures for its member countries. 'Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures' lays out the European Community's approach to electronic signature legislation. Of particular interest is Article 7, International Aspects, which recognizes the legal validity of digital certificates issued in a non-European Community country. *While international recognition of electronic signatures is important, there is concern that this approach will not recognize non-certificate based electronic signatures, such as those based on biometric technologies. The conference report notes that negotiations with the European Union on electronic signatures is a top priority.*[75]

The above might not be a fully accurate characterization of the referenced statutes.[76] Even so, it expresses a concern that is legitimate, to wit, that various countries will enact legislation recognizing only a particular kind of electronic signature or attribution procedure (authentication technology) and bar all others. The adverse impact on global electronic commerce is obvious. While private parties and governments may wish to require use of particular technologies for certain purposes—such as enhancing the accuracy of certain records or the like—in general the intention of E-Sign is to leave such determinations to private parties. Senator Leahy explained this concept of technology neutrality as follows:

> Finally, I want to discuss the concept of technology neutrality that is so central to this bill. *This legislation is, appropriately, technology neutral.* It leaves it to the parties to choose the authentication technology that meets their needs. At the same time, it is undeniable that some authentication technologies are more secure than others.

---

75. Abraham Statement of June 16, 2000, *supra* note 36, at S5288 (emphasis added).

76. For example, other sources describe the German digital signature law as setting technical standards for a PKI infrastructure but as not containing any legal consequences that derive from the use of PKI. *See* AALBERTS & VAN DER HOF, *supra* note 15, § 3.2.1.1, at 25–26 (Nov. 1999) (analyzing various international legislative approaches to the problem of electronic signatures).

> *Nothing in the conference report prevents or in any way discourages parties from considering issues of security when deciding which authentication technology to use for a particular application. Indeed, such considerations are wholly appropriate.*

Pursuant to the Government Paperwork Elimination Act, passed by the previous Congress, the Office of Management and Budget (OMB) has adopted regulations to permit individuals to obtain, submit, and sign government forms electronically. These regulations direct federal agencies to recognize that different security approaches offer varying levels of assurance in an electronic environment and that deciding which to use depends first upon finding a balance between the risks associated with the loss, misuse or compromise of the information, and the benefits, costs, and effort associated with deploying and managing the increasingly secure methods to mitigate those risks.

> The OMB regulations recognize that among the various technical approaches, in an ascending level of assurance, are "shared secrets" methods (e.g., personal identification numbers or passwords), digitized signatures or biometric means of identification, such as fingerprints, retinal patterns and voice recognition, and cryptographic digital signatures, which provide the greatest assurance. Combinations of approaches (e.g., digital signatures with biometrics) are also possible and may provide even higher levels of assurance.
>
> In developing this legislation, the conference committee recognized that certain technologies are more secure than others and that consumers and businesses should select the technology that is most appropriate for their particular needs, taking into account the importance of the transaction and its corresponding need for assurance.[77]

The U.S. approach, which is one that allows and encourages all technologies, recognizes the reality that technologies differ, and that no technology developed yet is foolproof—even with the high level of security made possible with public encryption.[78] Any

77. 146 CONG. REC. S5222–23 (daily ed. June 15, 2000) (statement of Sen. Leahy) (emphasis added).

78. For example, any inability to break an encryption key itself is not determinative if other problems exist. To illustrate, in September, 1995, two graduate students at the University of California at Berkeley posted a message on the Internet stating that the random number used by Netscape to generate the encryption key was "fairly trivial to guess" and that, in two days, they had discovered the number and written a software program that could guess the key in less than one minute. Jarad Sandberg, *Netscape's Internet Software Contains Flaw That Jeopardizes Security of Data*, WALL ST. J., Sept. 19, 1995, at A5. While Netscape was able to fix the problem, the example illustrates the

reading of the literature will illustrate drawbacks and concerns with every technology. Also, it is important not to require a high level of technology for every transaction simply because that technology may be available, as this would do more to burden e-commerce than to enable it, and such legislation would not be commensurate with the risks involved. A report surveying international approaches to the question of technology-neutral versus technology-specific legislation explains as follows:

> Moreover it is important to note that technologies may differ as to their reliability and security and not in every instance the highest reliability and security level will be required. There is a tendency of requiring higher levels of reliability than is necessary for the purposes to be served and often policy makers and legislators seem to lose sight of the fact that hand-written signatures were never that reliable either, rather on the contrary. Demanding higher reliability requirements merely because it is possible, would be a major (and unjustified) impediment to the development of e-commerce.[79]

Accordingly, any legal regime that adopts only one solution is bound, under the U.S. view, to fall victim to either the flaws in the adopted technology or to a refusal by commercial or consumer parties to embrace the technology and its consequences.

The United States is not alone in this view. The foregoing study labels UCITA and UETA as examples of the "technology neutral," or "minimalist" approach.[80] The study was completed before the enactment of E-Sign, but given E-Sign's reliance on UETA and UETA's reliance on the relevant provisions of UCITA, E-Sign too falls into this category. The study also cites the UNCITRAL Model Law on Electronic Commerce as an example of this approach,[81] which is not surprising given that UCITA and UETA draw from it. The study also cites the Australian Electronic Commerce Framework Bill of the State of Government of Victoria as an example of this approach.[82]

---

variety of possible security issues. Further, in testimony before a Senate panel in June, 1996, Philip Zimmerman, chairman and chief technology officer of PGP, Inc. (Pretty Good Privacy), said that, based on a 1993 presentation of Northern Telecom, a special machine could be built for $1 million that in 7 hours would try every possible DES key and, on average, crack a 56-bit code key in 3.5 hours. *Witness Tells Senate Codes Encrypted With 56-Bit DES Can Be Readily Cracked*, 67 BANKING REPORT (BNA) No. 2, 54, 54–55 (July 8, 1996). A more powerful machine, costing $10 million, would take 21 minutes to crack the key, while a $100 million machine could do it in 2 minutes. *Id*.

79. AALBERTS & VAN DER HOF, *supra* note 15, § 2.1, at 13–14 (footnotes omitted).

80. *Id*. § 4.4.2.2, at 53–54.

81. *Id*. § 3.2.3.1, at 36.

82. *Id*. § 3.2.3.2, at 38.

Regarding technology-neutrality, the authors of the report state that "[a] more technology-neutral approach will most likely be better suited to deal with future technologies than legislation that focuses solely on a specific technology."[83] They also note that legislation seems to be straying from the technology-specific approach and discuss a "two-prong" approach, which is legislation setting a certain minimum legal status for all electronic authentications and then assigning greater legal effect to certain technologies (secure electronic signatures).[84] They cite the UNCITRAL Draft Uniform Rules on Electronic Signatures as an example of this approach, as well as the EU Directive for Electronic Signatures.[85]

The report concludes, however, that the technology-neutral, or minimalist approach illustrated by UCITA appears to be the way to go:

> [W]e feel it is unwise to issue detailed regulations and to determine specific business models, such as the PKI model, when it is by no means clear, whether they turn out to be viable models. Viewed in this light, the digital signature approach is seriously flawed. Although the legislators and regulators under the digital signature approach may have done so for all the right reasons (legal certainty, trustworthiness with respect to legal matters), the approach as such is not recommendable . . . .
>
> The same is true, but to a lesser extent for the two-prong approach. The two-prong approach attempts to skirt around these problems by presenting an opening for new technologies besides setting criteria for certain advanced electronic signatures . . . . Still, within the two-prong approach legislation often deals with issues and situations (e.g., CAs, liability, qualities that focus mainly on certain techniques) which have not yet been determined and thus, may well need adjustment . . . .
>
> As far as we are concerned, we are back to our starting point with the minimalist approach taken in the UNCITRAL Model Law still offering the most sensible solution to legislators wanting to tackle the problem of formal requirements in their legislation.[86]

In short, they endorse the U.S. approach reflected in E-Sign, UCITA, and UETA.

83. *Id*. § 2.2.3, at 18.
84. *Id*. § 3.2.2, at 29.
85. *Id*. § 3.2.2.1–3.2.2.2, at 30–31.
86. *Id*. § 3.2.4, at 40–42 (footnotes omitted).

III. ATTRIBUTION OF SIGNATURES—ARE PARTICULAR TECHNOLOGIES REQUIRED?

A. What is An Attribution Procedure and Why is It Needed?

The Achilles heel of e-commerce is attribution. An "attribution procedure" is a procedure to verify that an electronic signature, message, or record is that of the person purporting to provide it.[87] An attribution procedure answers the essential e-commerce question: "in a contract purporting to be with Joe User, who clicked the 'I Agree' button?"—Joe, the dog, or a hacker? An attribution procedure can also be a procedure to detect changes or errors in information.[88]

Restated, this problem is how to prove that the person clicking "I Agree" really is the person with whom the "clickee" believes it is contracting. This is vividly illustrated in *Federal Trade Commission v. Verity International, Ltd.*,[89] in which the court determined that telephone line subscribers were not liable for calls made from the subscriber's number unless the biller for online services could prove that the subscriber was the person who consented to the online contract—in other words, the subscriber was the person who clicked "I Accept."[90] The "filed rate doctrine" usually supplies contracts and attribution procedures for telecommunications services through tariff rules—but the service in this case, viewing a "sexually oriented" Web site, was not subject to tariffs, so no "automatic" contracts or rules applied.[91] The service provider had to rely on private contracts—just like other providers of e-commerce services. The case illustrates the need to be able to prove who clicked.

How can one do that? Is there a law explaining how attribution can or cannot be done? No. E-Sign does not do so. Both UETA and UCITA describe attribution procedures,[92] and both honor contracts for them, but neither establishes what they must or cannot be. In E-Sign, the attribution concept is

87. UCITA § 102(a)(5) (2000).

88. *Id*.

89. 124 F. Supp. 2d 193 (S.D.N.Y. 2000).

90. *Id*. at 202 (reasoning that if a contract is formed by clicking "I accept," it only binds the person who clicked, and the telephone line subscriber is not automatically that person).

91. *Id*. at 200–02 (explaining that telephone line subscribers are routinely held responsible for phone calls they never authorized because they are presumed to have knowledge of the filed telephone rates and customer obligations).

92. UETA § 2(14) (1999) (providing the definition of "security procedures," the UETA term for an attribution procedure); UCITA § 102(15) (defining attribution procedure).

referenced as an "authentication" approach,[93] a term that seems to be loosely and variously used to refer to the integrity of a record or attribution to a person—maybe.

No matter the name, one purpose of the game is the same—to find a way to attribute consent. Each statute leaves the answer on how to do that to the parties. This is wise given that the circumstances will vary considerably and, thus, it is likely not possible to draft a "one-size-fits-all" rule—or at least one that would be acceptable at this stage in e-commerce. Early drafts of UCITA attempted to create a more directive rule by requiring that the attribution procedure be commercially reasonable. This approach stemmed from Article 4A of the U.C.C. but was not acceptable to proponents of the approach taken in UETA, an approach that allows the contract to govern regardless of commercial reasonableness.[94] At the annual meeting of the NCCUSL at which UCITA was approved, a vote was taken to revise UCITA to parallel UETA.[95] Accordingly, the statutory requirement for commercial reasonableness as a condition to attribution was intended to be removed.[96]

What is an attribution procedure? UCITA provides this helpful definition:

> "Attribution procedure" means a procedure to verify that an electronic authentication, display, message, record, or performance is that of a particular person or to detect changes or errors in information. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment.[97]

But what procedure should be adopted? The Department of the Treasury has listed various alternatives in its Electronic Authentication Policy, which is part of its implementation of the

93. E-Sign § 102(a)(2)(A), 15 U.S.C. § 7002(a)(2)(A) (2000); 104(b)(2)(C), 15 U.S.C. § 7004(b)(2)(C); 301(a)(2), 15 U.S.C. § 7031(a)(2).

94. U.C.C. §§ 4A-201, 4A-202(b)–(c) (establishing that banks may use any commercially reasonable security procedure to verify customers' payment orders); UETA § 7 (giving legal effect to electronic records, signatures, and contracts, without requiring commercial reasonableness).

95. U.C.C. §§ 4A-201, 4A-202(b)–(c).

96. Despite this vote and removal of the primary sections regarding commercial reasonableness, stray references remain which, given the vote and the comments (*see* for example, Official Comment No. 2 to UCITA § 212), should be interpreted not to require commercial reasonableness. However, unlike UETA, which is merely procedural, UCITA does require conscionability for all contract terms, including attribution terms. UCITA § 111 (2000).

97. UCITA § 102(a)(5).

Government Paperwork Elimination Act (GPEA).[98] The GPEA is *not* the same as E-Sign, UETA or UCITA, but the Policy's list of current attribution methods is nevertheless interesting:

> Knowledge based authentication, or shared secrets, such as PINs and passwords;
>
> Biometrics, such as fingerprint, voice, and eye characteristics;
>
> Secure tokens, such as smart cards;
>
> Cryptography, including digital signatures, challenge-response protocols (e.g., the "handshake" protocol in Secure Sockets Layer), and message authentication codes;
>
> Digitized signatures, including digital images of handwritten signatures and signature dynamics (i.e., measurements of the direction, pressure, speed, and other attributes of a handwritten signature).
>
> These electronic authentication techniques provide varying levels of security and non-repudiation. In practice, however, a robust authentication system will make use of multiple techniques in combination, such as the use of a PIN to unlock and apply a digital signature private key held on a smart card. While the scope of this policy is limited to payment, collection, and collateral transactions, these techniques may be applied to other types of financial transactions conducted over open networks, such as secure remote access to financial systems, and transmission of accounting data.[99]

Another U.S. agency, the Office of Management and Budget, has described the principle of balancing the risks of an insecure transaction with the costs associated with implementing security procedures in its guidance for the Government Paperwork Elimination Act:

> Combinations of approaches (e.g., digital signatures with biometrics) are also possible and may provide even higher levels of assurance than single approaches by themselves. *Deciding which to use in an application depends first upon finding a balance between the risks associated with the loss, misuse, or compromise of the information, and the benefits, costs, and effort associated with deploying and managing the increasingly secure methods to mitigate those risks.*

98. Electronic Authentication Policy, 66 Fed. Reg. 394 (Jan. 3, 2001) (advancing policies and practices to be followed by agencies when making federal payments and collections electronically over open networks such as the Internet).

99. *Id*. at 2,394–95.

> *Agencies must strike a balance, recognizing that achieving absolute security is likely to be highly improbable in most cases and prohibitively expensive if possible.*[100]

How will all of this work in the real world? A hint may be available in *United States v. Siddiqui*,[101] a criminal case. The defendant was convicted of making fraudulent and false statements to a federal agency and obstructing a federal investigation.[102] He was a visiting professor at the University of Alabama who desired to win the Waterman Award, a $500,000 prize awarded by the National Science Foundation (NSF) to an outstanding scientist or engineer.[103] The NSF received nomination or recommendation forms from two scientists who later noted that they had never made the nomination or recommendation.[104] Turns out, the defendant had nominated himself but claimed he had permission from the scientists.[105] The defendant objected to the admission into evidence of several emails, including: (1) one purportedly from the defendant asking one of the scientists to back defendant up if the NSF called; the email was signed "Mo"—the defendant's nickname—and had defendant's address as the "sender's" address; (2) one asking the scientist to say that she had authorized defendant to submit the nomination on her behalf—she also received a phone call making the same request and she recognized defendant's voice; and (3) an email to the other scientist, showing defendant as sender, asking the scientist to back defendant up—during the same time, that scientist also received a phone call and recognized defendant's voice.[106]

The Federal Rules of Evidence require documents to be properly authenticated as a condition of admissibility "by evidence sufficient to support a finding that the matter in question is what its proponents claim."[107] The court cited precedent holding that a document may be authenticated by "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances," including circumstantial

100. OFFICE OF MANAGEMENT AND BUDGET, IMPLEMENTATION OF THE GOVERNMENT PAPERWORK ELIMINATION ACT, http://www.whitehouse.gov/OMB/fedreg/gpea2.html (emphasis added).

101. 235 F.3d 1318 (11th Cir. 2000).

102. *Id*. at 1320.

103. *Id*.

104. *Id*. at 1320–21.

105. *Id*. at 1320.

106. *Id*. at 1321–22.

107. FED. R. EVID. 901(a).

evidence.[108] In this case, the court found that the following factors supported the authenticity of the emails:

- ?? each bore the defendant's email address at the university;
- ?? that address was the same as an email sent to the defendant by one of the scientists—and that was introduced by defendant's counsel to show permission to submit the nomination;
- ?? one scientist testified that, when he replied to the email apparently sent by defendant, the "reply-function" on his system automatically dialed defendant's email address as the sender;
- ?? the context of the email sent by defendant showed the author was someone who knew the very details of defendant's conduct with respect to the award and investigation;
- ?? in one email sent to one of the scientists, the author made apologies for leaving early from a meeting attended by that scientist and the defendant;
- ?? the emails used the defendant's nickname;
- ?? both scientists spoke on the phone with the defendant soon after receipt of the emails and the defendant made the same request as made in the emails.[109]

Given the above, the appellate court concluded that the district court had not abused its discretion in admitting the emails.[110] The point of this discussion is to illustrate that, even without encryption or other sophisticated authentication factors, electronic documents can be and are being authenticated.

B. Technological Neutrality for Attribution

What if a state wanted to enact legislation requiring use of a particular technology for attribution. May it do so? The answer appears to be "no." As discussed in Part II, *supra*, the answer is a clear "no" with respect to electronic signatures themselves.[111] But take another look at section 102 of E-Sign—it applies to electronic signatures *and* authentication (in this sense, meaning attribution) of records or signatures:

---

108. *Siddiqui*, 235 F. 3d at 1322 (quoting FED. R. EVID. 901(b)(4) and citing United States v. Smith, 918 F.2d 1501, 1510 (11th Cir. 1990)).

109. *Id*. at 1322–23.

110. *Id*. at 1323.

111. Refer to Part II *supra*.

> SEC. 102. EXEMPTION TO PREEMPTION.
>
> (a) IN GENERAL.—A State statute, regulation, or other rule of law may modify, limit, or supersede the provisions of section 101 with respect to State law only if such statute, regulation, or rule of law—
>
> . . . .
>
> (2)(A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, *if*—
>
> (i) such alternative procedures or requirements are consistent with this title and title II; and
>
> (ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, *or authenticating electronic records* or electronic signatures. . . .[112]

The same theme is repeated in section 301 of E-Sign regarding the approach the United States will take internationally:

> SEC. 301. PRINCIPLES GOVERNING THE USE OF ELECTRONIC SIGNATURES IN INTERNATIONAL TRANSACTIONS.
>
> (a) PROMOTION OF ELECTRONIC SIGNATURES.
>
> (1) REQUIRED ACTIONS.—The Secretary of Commerce shall promote the acceptance and use, on an international basis, of electronic signatures in accordance with the principles specified in paragraph (2) and in a manner consistent with section 101 of this Act. The Secretary of Commerce shall take all actions necessary in a manner consistent with such principles to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and foreign commerce.
>
> (2) PRINCIPLES.—The principles specified in this paragraph are the following:

112. E-Sign § 102(a)(1)–(2), 15 U.S.C. § 7002(a)(1)–(2) (2000) (emphasis added).

. . . .

> (B) Permit parties to a transaction to determine the appropriate *authentication technologies* and implementation models for their transactions, *with assurance that those technologies and implementation models will be recognized and enforced*.
>
> (C) Permit parties to a transaction to have the opportunity to prove in court or other proceedings *that their authentication approaches* and their transactions *are valid*.
>
> (D) Take a nondiscriminatory approach to electronic signatures *and authentication methods from other jurisdictions*.[113]

That the term "authentication" is used in this context to mean attribution, is indicated not only by the wording but also by Congressional comments. For example, focus again on the comments made by Senator Leahy accompanying note 77 of this Article. His statement can as easily be applied to attribution technologies as signature technologies.

In short, E-Sign appears to require technological neutrality not only for the e-signature itself, but also for the attribution procedure used to tie the signature to a particular person. E-Sign expressly restricts regulators from requiring particular technologies or technical specifications for performing "the functions of creating, storing, generating, receiving, communicating, or *authenticating electronic records* or electronic signatures."[114] Although E-Sign does allow federal or state regulatory agencies to "specify performance standards to assure accuracy, record integrity, and accessibility of the records that are required to be retained"—this exception does not appear to include attribution of signatures.[115]

C. Example of Attribution Procedure, Albeit Misleading

One federal regulator has attempted to supply guidance on attribution procedures concerning particular e-transactions with the federal government. It provides an example of how to analyze levels of risk and then determine a procedure. It is misleading for our purposes, however, because it is not technologically neutral and, thus, would not be appropriate for use in a transaction subject to E-Sign. But it is nevertheless interesting.

---

113. *Id.* § 301(a), 15 U.S.C. § 7031(a) (emphasis added).
114. *Id*. § 104(b)(C)(iii), 15 U.S.C. § 7004(b)(2)(C)(iii) (emphasis added).
115. *Id*. § 104(b)(3)(A), 15 U.S.C. § 7004(b)(3)(A).

The example is provided by the Department of the Treasury's "Electronic Authentication Policy" ("Policy").[116] The Policy is part of the Treasury's implementation of the Government Paperwork Elimination Act (GPEA).[117] The Policy is of interest because it is one of the first indications of what would be acceptable to the government, at least in the foregoing transactions and under the GPEA.[118] *It is critical to note that the Policy cannot be applied broadly, even by analogy*, because it is issued under the GPEA and that act is *not* subject to section 104(a) or (b) of E-Sign.[119] In short, the government has more leeway under the GPEA to issue mandates regarding particular technologies, and what might be acceptable under GPEA may well be illegal under E-Sign.

The Policy deals with procedures and practices to be followed by agencies when making federal payments and collections electronically over open networks like the Internet.[120] It also covers certain collateral transactions such as electronic messages or instructions to pledge, deposit, release, or claim collateral used to secure public funds.[121] "These payment, collection, and collateral transactions may be between the federal government and non-Federal entities, as well as transactions between federal entities."[122] In particular, the Policy addresses the authentication of the identity of parties to such transactions.[123]

The Policy does not apply to transactions over closed networks such as: financial networks owned or controlled by the government, the federal reserve, or private financial institutions. It pertains only to open networks.[124] The Policy does not dictate providers, although it does favor certain account holding institutions, and the background discussion for the Policy expressly states that, while it sets forth a model or guidance for determining the robustness of electronic authentication for particular types of transactions, it does *not* dictate a specific technique or system—except with respect to certain high risk

116. Electronic Authentication Policy, 66 Fed. Reg. 2,394 (Jan. 3, 2001).

117. *Id*.

118. *Id*.

119. *See* E-Sign § 104(c)(2), 15 U.S.C. § 7004(c)(2) (noting that the federal government is not relieved of its obligations under the GPEA).

120. 66 Fed. Reg. 2,394–95 (Jan. 3, 2001).

121. *Id*.

122. *Id*. at 2,394.

123. *Id*.

124. *Id*. at 2,394–95 (explaining that authentication concerns are greater with open networks because access is unrestricted, unlike government owned or controlled closed networks).

transactions.[125]

What is the Policy? It is affected by defined terms and complexities, but a basic concept is that "[a]ll payment, collection, and collateral transactions must be properly authenticated, *in a manner commensurate with the risks of the transaction*."[126] The three basic risks to be assessed are: (1) monetary loss; (2) reputation risk; and (3) productivity risk—and the Policy provides guidance on how the Treasury believes those risks should be assessed.[127] The Electronic Authentication Policy differentiates between transactions on the basis of risk:

> For purposes of federal payment, collection, and collateral transactions, there are four risk categories: high, moderate, low, and negligible. The risk category indicates the robustness of the electronic authentication technique that must be used . . .[the policy notes that the] [h]igh and moderate risk transactions require multi-factor authentication, where at least two electronic authentication techniques must be used in combination, such as digital signature with a PIN [personal identification number] protecting the signing key.
>
> (1) High Risk.
>
> (A) Multi-factor authentication is required, including a digital signature.
>
> (B) Private cryptographic keys must be generated, stored, and used in a secure cryptographic hardware module.
>
> (C) Certification authorities must operate under the Government's direct policy authority.
>
> (2) Moderate Risk.
>
> (A) Multi-factor authentication is required.
>
> (B) Private cryptographic keys may be stored in software.
>
> (C) Certification authorities which are under the policy authority of a commercial entity meeting the requirements of this policy may be used.
>
> (3) Low Risk. Single factor authentication must be used, such as a PIN or a software based SSL client certificate.
>
> (4) Negligible Risk. Transactions may occur without an

125. *Id*.

126. *Id*. at 2,396 (emphasis added).

127. *Id*.

electronic authentication technique.[128]

Would the Policy work effectively in e-commerce generally even if it were legal under E-Sign? Any policy requiring a particular technology will have to pass muster under E-Sign, and commercial and consumer users must be willing to accept it. In the end, the requirements for digital signatures may prove to be too strong, or not commercially acceptable for general e-commerce, or too strong in light of risks in non-electronic commerce that are not similarly addressed. But no one knows how it will all turn out.

IV. CONSUMER CONSENT RULES FOR DELIVERY OF E-DISCLOSURES

A. The Rule Generally

The purpose of E-Sign is to enable electronic commerce. E-Sign section 101(c) ("Subsection (c)") recognizes, however, that federal and state laws include specific, preliminary policy decisions intended to protect consumers by requiring delivery in writing of particular notices or disclosures to consumers.[129] In Subsection (c), "writing" means "on paper." Thus, E-Sign's consumer consent rule, discussed in this section, reflects a policy to ensure that disclosures are actually made—oral disclosures are susceptible to arguments over whether the disclosure was made and over what actually was said. If a disclosure must be delivered on paper, those arguments end and the consumer also may keep the copy when one must be delivered. How should those kinds of statutes be handled in an electronic age? Is it appropriate to allow such disclosures to be delivered electronically?

The Subsection (c) answer is "yes," as long as the prior consent of the consumer is obtained and extensive disclosures are made.[130] This is likely overkill and will seem odd in future years, but E-Sign provides uniform rules while also allowing regulatory reconsideration of the rules' advisability. The tension E-Sign sought to address, and the fact that not all of the assumptions made in it may be accurate, can be explained as follows:

> In a digital economy, the idea that agreements to use digital messages require special formalities would be

128. *Id*.

129. *See* E-Sign § 101(b)(1), 15 U.S.C. § 7001(b)(1) (2000).

130. *Id*. § 101(c)(1)(A)–(B), 15 U.S.C. § 7001(c)(1)(A)–(B) (allowing electronic disclosures to be substituted for written disclosures after the consumer is provided with the specific disclosures listed in E-Sign).

> absurd if it were broadly applied. As we have seen, however, the intent in the E-Sign Act is that the disclosure and consent rules apply only where a consumer protection law requires disclosures in writing. The argument thus narrows to the belief that such a specific policy decision about written disclosures or notices should not be dislodged easily by a general validation statute. A state might, however, amend its own consumer protection laws to broadly accept electronics as equivalent to paper. Five years from now, the idea that they are not will seem quaint. A few years after that, the restrictions will be repealed, ignored, or viewed as a barrier to electronic commerce. The comments of Senator Phil Gramm make this point nicely:
>
> "There are those who are fearful of the electronic market place, and that fear found its expression in the debates in the conference committee. It found its expression in provisions in this bill that apply standards to electronic commerce that are not applied to paper commerce. That is not unusual. Every major technological advance has met with fear before its full benefits were embraced. It may seem odd, but not over one hundred years ago there was a very spirited congressional debate about whether it was safe to buy an automobile for transporting the President. Voices were loudly raised in Congress that automobile transportation was not safe, that it was too risky to let the President be transported in anything other than a horse-drawn carriage. Governments passed restrictions on automobile use that seem silly to us today. I believe that many of the fears that have been raised about electronic commerce will very soon sound silly. In fact, many of them do not make much sense today. That is why I am pleased that this legislation will allow the regulators to remove many of these onerous restrictions if the fears prove unfounded, as I expect that they will . . . . Electronic commerce should labor under no greater regulatory restrictions than does the quill pen, if this is to be a system for the twenty-first century."[131]

In any case, Subsection (c) is a reality for now, and the first step to understanding it is to determine to what kinds of statutes it applies. An example is the federal Truth in Lending Act, which is implemented by Regulation Z.[132] In consumer credit transactions, 12 CFR § 226.17 establishes this rule for certain kinds of credit:

> (a) *Form of disclosures.* (1) The creditor shall make the

131. Nimmer, *supra* note 45, at 18–19.

132. Truth in Lending (Regulation Z), 12 C.F.R. § 226 (2001) (requiring creditors to make certain required disclosures to consumers, many of which must be in writing).

> disclosures required by this subpart clearly and conspicuously in writing, in a form that the consumer may keep. The disclosures shall be grouped together, shall be segregated from everything else, and shall not contain any information not directly related to the disclosures required under § 226.18.[133]

Regulation Z is an example of a statute to which Subsection (c) applies. It is a consumer protection statute, other than E-Sign, which requires that a disclosure or notice of information be provided in a writing on paper *to* a consumer; it does not require anything *from* a consumer.[134] Such disclosures are referenced in this article as the "Consumer Protection Statute Disclosure Statement." E-Sign, subsection (c)(1)(B), itself requires a disclosure statement,[135] and this Article refers to that disclosure as the "E-Sign Disclosure Statement." One must think in terms of *two* different disclosure statements to understand Subsection (c).

If a person who is supposed to provide the Consumer Protection Statute Disclosure Statement desires to provide it in electronic form instead of on paper, Subsection (c) generally requires that person to do the following:

- Provide a clear and *conspicuous* E-Sign Disclosure Statement of, among other items, the hardware and software required to access the Consumer Protection Statute Disclosure Statement, and the procedures for—and consequences of—withdrawing consent to receive the Consumer Protection Statute Disclosure Statement electronically.[136]

- *After* providing the E-Sign Disclosure Statement, obtain *electronically* the consumer's *affirmative* consent (or confirmation of his consent) to receive the Consumer Protection Statute Disclosure Statement electronically.[137]

- This consent (or confirmation of consent) must be obtained in a manner that *reasonably demonstrates* that the consumer can access the Consumer Protection Statute Disclosure Statement in the electronic form

133. *Id*. § 226.17(a) (footnote omitted) (emphasis added).

134. *Id*. § 226.5(a), 226.16(a).

135. E-Sign § 101(c)(1)(B), 15 U.S.C. § 7001(c)(1)(B) (2000). Subsection (c) only applies to written information that must be provided *to* a consumer. *Id*. § 101(c)(1), 15 U.S.C. § 7001(c)(1).

136. *Id*. § 101(c)(1)(B)–(C), 15 U.S.C. § 7001(c)(1)(B)–(C).

137. *Id*. § 101(c)(1)(A), (c)(ii), 15 U.S.C § 7001(c)(1)(A), (c)(ii).

used to provide it.[138]

?? If a change in the hardware or software creates a material risk that the consumer won't be able to access the Consumer Protection Statute Disclosure Statement, then a new E-Sign Disclosure Statement has to be provided and the consent and reasonable demonstration steps have to be done again.[139]

In addition, the appropriate requirements of the regulator in charge of the underlying consumer protection statute must be met.[140] The actual wording of Subsection (c) is included in Appendix II of this Article.[141] This paper will focus on the basic elements of the rule—see Appendix II for disclosure details.

B. Elements of the Rule

The first paragraph of Subsection (c) is the most important because it determines whether application of Subsection (c) is even triggered. Almost every word must be considered, but among the basic issues to consider are the following:

1. Consumer: Is there any law other than E-Sign requiring *provision of information to a consumer (delivery of a Consumer Protection Statute Disclosure Statement)?* A consumer is defined in E-Sign as "an *individual* who obtains, through a transaction, products or services which are *used* primarily for personal, family, or household purposes, and also means the legal representative of such an individual."[142] A legal entity is not a "consumer." While "individual" is not defined in E-Sign, the term is used in federal and state legislation to mean a human being.[143]

---

138. *Id*. § 101(c)(1)(C), 15 U.S.C. § 7001(c)(1)(C).

139. *Id*. § 101(c)(1)(D), 15 U.S.C. § 7001(c)(1)(D).

140. For proposed rules of the Federal Reserve Board on implementing standards for delivering disclosures to consumers under five consumer protection statutes, *see* Equal Credit Opportunity (Regulation B), 12 C.F.R. § 202 (2001); Electronic Fund Transfers (Regulation E), 12 C.F.R. § 205 (2001); Consumer Leasing (Regulation M), 12 C.F.R. § 213; Truth in Lending (Regulation Z), 12 C.F.R. § 226 (2001); Truth in Savings (Regulation DD), 12 C.F.R. § 230 (2001).

141. Refer to Appendix 2 *infra* (providing the text of subsection (c)).

142. *Id*. § 106(1), 15 U.S.C. § 7006(1).

143. For example, the federal Dictionary Act lists "individuals" as a subcategory of "person," apparently referring to human beings, while "person" refers to both individuals and artificial persons such as corporations and other entities. Dictionary Act of 1947, 1 U.S.C. § 1 (1994). Section 106(8) of E-Sign defines "person" as "an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity." E-Sign § 106(8), 15 U.S.C. § 7006(8). The NCCUSL also defines "person" as including both natural persons and other entities and reserves "individuals" for human beings. *See, e.g.*, UCITA § 102, cmts. 13, 45 (2000). Furthermore, under U.S. bankruptcy

The E-Sign definition looks to "use" of the product or service. One of the primary E-Sign authors has indicated that E-Sign follows the traditional interpretation of "consumer" by looking to intent for use stated at the time of the transaction and not subsequent, actual use:

> To clarify further the definition of "consumer," the definition is intended to be consistent with traditional interpretations of such definitions. *This means that the party dealing with the consumer may rely on the consumer's intended use for the product or service as indicated when the transaction is entered into.* Thus if an individual indicates at the time of the transaction that the online purchase of a heater is primarily for personal family or household use, then that individual is a consumer; the fact that the individual may later dedicate the actual use of the heater to the individual's business is not relevant. The opposite is also true: if an individual indicates that the intended use is primarily for business purposes, then that individual is not a consumer even if the individual later uses the heater primarily for personal or family purposes.[144]

2. Required Writing: Is there a requirement in the law (other than E-Sign) for the information to be in a writing*?* Subsection (c) only applies to information that is *required* to be provided to a consumer *in writing*.[145] Not all statutes contain writing *requirements*; for example, Revised Article 9 of the U.C.C. requires many items to be in a "record" but, generally, that requirement can be met with either an electronic or non-electronic record.[146] Subsection (c) will never apply to a statute of that type because it

---

law, consumer debt means "[d]ebt incurred by an individual primarily for a personal, family, or household purpose"; while individual is not defined, a "person" includes individuals, partnerships, and corporations, but the definition of "corporation" does not include human beings, and "individual" and "partnership" appear to be mutually exclusive terms. *See In re* Circle Five, Inc., 75 B.R. 686, 688 (Bankr. D. Idaho 1987) (citation omitted). Therefore, a corporation is not an individual under the bankruptcy code. *Id*.

144. Abraham Statement of June 16, 2000, *supra* note 36 (emphasis added).

145. E-Sign § 101(c)(1), 15 U.S.C. § 7001(c)(1).

146. The Uniform Commercial Code Series (U.C.C.S.) states:

> Revised Article 9 is, generally speaking, medium neutral. It uses the term "record" rather than "writing" and the term "authenticate" rather than "sign" in order to accommodate those concepts to electronic, nonwritten modes of communication. Indeed, at some point in the future, electronic communication of electronic documents might replace physical delivery of written documents.

U.C.C.S. [Rev] § 9-521:1 (West 2001). In Revised Article 9, "'[r]ecord', except as used in 'for record', 'of record', 'record or legal title', and 'record owner', means information that is inscribed on a tangible medium or which is stored in an electronic or other medium and is retrievable in perceivable form." U.C.C. § 9-102(a)(69) (2001).

does not *require* anything to be delivered to consumers in a *writing*. As explained by the Office of Management and Budget with respect to E-Sign generally:

> E-SIGN applies broadly to commercial, consumer, and business transactions affecting interstate or foreign commerce, and to transactions regulated by both Federal and state government. *If there is no writing required by another law, E-SIGN does not apply*.[147]

The FTC telephone-mail order rule is an example of a disclosure statute that is not subject to Subsection (c) because the telephone-mail order rule, which requires the provision of information (notice about shipment delays), does not require that the information be in writing.[148] Accordingly, and for that reason alone, it does not trigger Subsection (c).

Note that under E-Sign, "writing" refers to paper writing requirements, that is, state or federal laws that require delivery of *paper* notices or disclosures to consumers.[149] In future years, as "writing" becomes more widely assumed to mean anything with legible characters[150]—whether non-electronic or electronic—this

147. OFFICE OF MANAGEMENT AND BUDGET, GUIDANCE ON IMPLEMENTING THE ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT (E-Sign) at 2 (2000) [hereinafter E-Sign Guidance] (emphasis added), *available at* http://www.whitehouse.gov/omb/memoranda/e-sign-guidance.pdf.

148. *See* 16 C.F.R. § 435.1(b)(i) (2001) (requiring notice, but not written notice, of shipping delays).

149. Abraham Statement of June 16, 2000, *supra* note 36 ("[I]f a consumer protection statute requires delivery of a paper copy of a disclosure . . . then the consent and disclosure requirements of subsection (c)(1)(A)–(D) must be satisfied. Otherwise, subsection (c) does not disturb existing law.").

150. *See, e.g.*, *In re* RealNetworks, Inc., Privacy Litigation, No. 00 C 1366, 2000 WL 631341, at *1–3 (N.D. Ill. May 8, 2000) (finding that a state law "writing" requirement allows electronic writings). A law such as this would not trigger Subsection (c). *In re RealNetworks* involved RealNetworks' online license for RealPlayer and RealJukebox, software enabling plaintiffs to play and record Internet music. *Id*. at *1. Plaintiffs alleged trespass and privacy violations (alleging that the software secretly allowed RealNetworks to access their communications) and objected to enforcement of an arbitration clause on grounds, among others, that the federal and Washington State arbitration acts required arbitration provisions to be in a "writing." *Id*. at *1–2. The court analyzed the argument as follows:

> Both the Intervenor and RealNetworks agree that Congress intended the FAA [Federal Arbitration Act] to apply only to written contracts. Because the terms in the statute must be given their plain meaning and do not explicitly allow for an "electronic" agreement, Intervenor reasons that an electronic communication cannot satisfy the writing requirement, but only a written one can. However, this only begs the question, what is a written agreement? Although contract terms must be given their plain and ordinary meaning, the Court is unconvinced that the plain and ordinary meaning of "writing" or "written" necessarily cannot include any electronic writings. . . .
>
> Courts frequently look to dictionaries in order determine the plain meaning of words and particularly examine how a word was defined at the time the

wording may become confusing. Perhaps the way to keep it straight is to remember that, if in E-Sign "writing" referred to electronic writings, there would be no need for the E-Sign consumer consent rule at all, and its provisions would be nonsensical. One does not need consumer consent to receive a "written" disclosure electronically if "written" already includes electronic disclosures.

3. Information: Does the statute require delivery of information *to the consumer?* Not all writing requirements trigger Subsection (c). It only pertains if a statute, regulation, or other rule of law requires that *information* relating to a transaction in or affecting interstate or foreign commerce be provided or made available to a consumer in writing.[151]

E-Sign defines information similarly to UCITA. The E-Sign version defines information as "data, text, images, sounds, codes, computer programs, software, databases or the like."[152] The definition works well in UCITA where it helps to define the subject matter of the act—computer information transactions. The definition is, however, nonsensical in E-Sign where literal use of the definition is impossible. For example, what statute requires "computer programs" or "databases" to be made

statute was drafted and enacted. The FAA was enacted in 1925. . . . In relevant part, at the time, Webster's Dictionary defined "writing" as:

> 1. The act or art of forming letters or characters on paper, wood, stone, or other material, for the purpose of recording the ideas which characters and words express, or of communicating them to others by visible signs. 2. Anything written or printed; anything expressed in characters or letters.

Webster's defined "written" as the participle of write, which it defined as:

> 1. To set down, as legible characters; to form the conveyance of meaning; to inscribe on any material by a suitable instrument; as, to write the characters called letters; to write figures.

A legal dictionary at the time provided that "The word 'written,' used in a statute, may include printing and any other mode of representing words and letters. . . ." Thus, although the definition of a writing included a traditional paper document, it did not exclude representations of language on other media. Because electronic communications can be letters or characters formed on the screen to record or communicate ideas be [sic] visible signs and can be legible characters that represent words and letters as well as form the conveyance of meaning, it would seem that the plain meaning of the word "written" does not exclude all electronic communications. That being said, the Court does not now find that all electronic communications may be considered "written." Rather, the Court examines the contract at issue in this action and finds that its easily printable and storable nature is sufficient to render it "written."

In re RealNetworks, 2000 WL 631341, at *2–3 (internal citations omitted).

151. E-Sign § 101(c)(1), 15 U.S.C. § 7001(c)(1) (2000) (emphasis added).

152. *Id.* § 106(7), 15 U.S.C. § 7006(7). UCITA defines information as "data, text, images, sounds, mask words, or computer programs, including collections and compilations of them." UCITA § 102(a)(35) (2000).

available to a consumer in writing? The federal Office of Management and Budget describes what is meant by relying on the typical meaning of "information," that is, notices that are supposed to inform another person. The OMB describes Subsection (c) by explaining that "Federal, State, and local laws or rules require that parties receive *notices* and *disclosures* in connection with private transactions (for example real estate purchases and settlements). . . . E-SIGN establishes special requirements for the use of electronic *notices* and *disclosures* in consumer transactions."[153]

Subsection (c) should be read to apply to *disclosure* and *notice* statutes, which require delivery of information about a contract or other aspect of a transaction—such as Truth-in-Lending Act disclosure—as opposed to statutes requiring a contract, or term, itself *be in* a writing.

The E-Sign Act follows the more traditional approach in U.S. law and distinguishes between commercial and consumer cases.[154] It also focuses the consumer rules on the context to which the consumer concerns relate. Properly stated, consumer concerns primarily focus on disclosure and notice requirements, rather than contract formation; most consumer contracts do not require a signed writing for enforceability. The E-Sign Act recognizes this and, while it creates elaborate disclosure and consent rules, it does so only where consumer protection laws require that information be made available to a consumer in a writing. Typically these are disclosure or notice-giving rules.[155]

This is reiterated in two statements made by Senator Abraham, a primary author of E-Sign:

---

153. E-Sign Guidance, *supra* note 147, at 2 (emphasis added).

154. Nimmer, in discussing the definition of "consumer" in E-Sign said:

> The definition of consumer follows ordinary standards in U.S. law which are also followed in UCITA. It states: "The term 'consumer' means an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." E-Sign § 106(1). The legislative history further states: "This means that the party dealing with the consumer may rely on the consumer's intended use for the product or service as indicated when the transaction is entered into. Thus if an individual indicates at the time of the transaction that the online purchase of a heater is primarily for personal family or household use, then that individual is a consumer; the fact that the individual may later dedicate the actual use of the heater to the individual's business is not relevant. The opposite is also true: if an individual indicates that the intended use is primarily for business purposes, then that individual is not a consumer even if the individual later uses the heater primarily for personal or family purposes." Statement Concerning Conference Committee Report, Cong. Rec. S5287.

Nimmer, *supra* note 45, at 26 n.38.

155. *Id*. at 16.

> Section 101(c) honors the provisions of underlying law (except as to the specifics of writing and consent requirements); *the Act does not create new requirements for electronic commerce* but simply allows *disclosures* or other *items* to be *delivered* electronically instead of on paper. This means that if a consumer protection statute *requires delivery of a paper copy of a disclosure or item to a consumer*, then the consent and disclosure requirements of subsection (c)(1)(A-D) must be satisfied. *Otherwise, Subsection (c) does not disturb existing law*.
>
> *Section 101(c)(1) refers to writings that are required to be delivered to consumers by some other law, such as the Truth-in-Lending Act*. The reference to consumers is intentional . . . .[156]

Why analyze the above point? The answer is "statutes of frauds" and contract term formation statutes. Consider this statute of frauds:

> In the following cases . . . any agreement, contract and promise shall be *void*, unless such agreement, contract or promise, or some note or memorandum thereof, be in *writing*, and *signed* by the party to be charged therewith . . . : (1) Every agreement that by its terms is not to be performed in one year from the making thereof . . . .[157]

Under this kind of statute, is any *information* required to be *provided* or *made available*, to a consumer or anyone else, in writing? No. This kind of statute illustrates a contract *formation* statute, that is, a statute of frauds that renders void or unenforceable particular contracts that are not *in* a signed writing or do not *contain* certain information.[158] The writing requirement dictates whether or not the contract can exist or be enforced at all, not (a) whether *information* is disclosed, or (b) whether the contract is *delivered* to one or other of the parties. Under a statute of frauds analysis, the signed contract must merely *exist* at some point in time. This is an "existence" analysis, not a notice or disclosure concept, and not a "provide or make available" concept. Similar statutes also exist for some contract terms, that is, various statutes require particular terms to be *in* writing or the term cannot be enforced.[159] The policy behind such statutes is to preclude oral claims of contract, or of

156. Abraham Statement of June 16, 2000, *supra* note 36, at S5284.

157. WASH. REV. CODE § 19.36.010 (1999) (emphasis added).

158. *See, e.g., id*.

159. Refer to note 149 *supra*. The arbitration term in the case cited in the note was required to be in a writing to be enforceable.

particular contract terms. Thus, if one party intends to bind the other to certain contracts or terms, then the contract or term must be in writing—oral claims of agreement will not suffice.[160]

But these statutes of frauds or these "contract term formation" rules do not trigger Subsection (c). E-Sign would turn substantive law on its head if the "information" referenced in Subsection (c) were interpreted to apply to statutes of frauds or such other statutes, that is, if a consumer must be given the E-Sign Disclosure Statement before a contract "not to be performed within one year"[161] with the consumer can be made electronically. Not only would such a reading cause a dramatic change in substantive law—something that E-Sign does not purport to do—but no information is required to be "provided or made available" to anyone, let alone a consumer, under such statutes.[162] Accordingly, Subsection (c) should not be triggered. Given the importance of statutes of frauds and term formation statutes in contract law, as well as the importance of understanding whether E-Sign does or does not affect them, it is unfortunate that one has to parse Subsection (c) so carefully to reach the conclusion that Subsection (c) does not apply to them. A shorter road to that conclusion might be to try to write an E-Sign Subsection (c) disclosure statement for a statute of frauds: any effort to do so will illustrate that the resulting product is nonsensical.

There may be an additional reason that Subsection (c) does not apply to statutes of frauds or term formation statutes. As noted, Subsection (c) is only triggered when another statute *requires* that *information* relating to a transaction in or affecting interstate or foreign commerce be *provided or made available* to a *consumer* in writing.[163] A congressional statement suggests that use of the word "consumer" was intended to confine Subsection (c) to consumer protection statutes as opposed to generally applicable statutes that happen to pertain to consumers along with others:

---

160. E-Sign section 101(a) essentially converts requirements for such contracts or terms to be in a "writing" into a requirement that the contract or term be in an "authenticated record" or simply a "record." In other words, there must be some record, electronic *or* non-electronic, retrievable in perceivable form; depending upon the statute, that record must also be signed electronically *or* otherwise. Refer to text accompanying note 9 *supra*. The conversion does not disturb the policy behind statutes of frauds or similar statutes. There are still statutes of frauds but they can be met under the equivalency principle. Thus, electronic or non-electronic records and signatures work equally well but oral contracts remain unenforceable.

161. *See, e.g.*, WASH. REV. CODE § 19.36.010.

162. E-Sign § 101(c)(1), 15 U.S.C. § 7001(c)(1) (2000). *See, e.g.*, WASH. REV. CODE § 19.36.010 (lacking any requirement that anyone be provided with information).

163. E-Sign § 101(c)(1), 15 U.S.C. § 7001(c)(1) (emphasis added).

> Section 101(c)(1) refers to writings that are required to be delivered to consumers by some other law, such as the Truth-in-Lending Act. *The reference to consumers is intentional: Subsection (c) only applies to laws that are specifically intended for the protection of consumers. When a statute applies to consumers as well as to non-consumers, Subsection (c)(1) should not apply. In this way, the subsection preserves those special consumer protection statutes enacted throughout this Nation without creating artificial constructs that do not exist under current law.* At no time in the future should these "consent" provisions of 101(c), which are intended to protect consumers (as defined in this legislation), be permitted to migrate through interpretation so as to apply to business-to-business transactions.[164]

Consumer protections statutes are intended to provide special protections to consumers but not others. Contract or term formation statutes typically are not consumer protection statutes—they are statutes that apply to *all* contracts, including those made with consumers.[165] It is not necessary to rely on this reading of E-Sign, however, to reasonably conclude that Subsection (c) does not apply to statutes of fraud or term formation statutes. The E-Sign requirement that "information" be provided makes that point.[166]

*4. Delivery: Must the writing required by the consumer protection statute be "*provided or made available*" to the consumer?* Subsection (c) applies when the requisite information must be "provided or made available" to a consumer in writing, and the provider desires to substitute an electronic disclosure.[167] What does "provide or make available" mean? The answer, consistent with enabling e-commerce while not disturbing existing law or creating imbalances between electronic commerce and non-electronic commerce, is that this wording refers to statutes requiring a writing

164. Abraham Statement of June 16, 2000, *supra* note 36, at S5284 (emphasis added).

165. There are some statutes of frauds (or contract term formation statutes) that only apply in consumer transactions, but even then there typically is no requirement in the statute of frauds itself that the contract be provided or made available to a consumer. For example, a statute of frauds might state that in a consumer transaction, a contract of type X must be in signed writing. The statute does not also say that the contract must be delivered to a consumer. Typically, contracts are delivered to each party as a matter of practice, but it would be unusual for such a requirement to be contained in the statute of frauds because, as noted, it focuses on the *existence* or formation of certain contracts, rather than on who gets the writing.

166. E-Sign § 101(c)(1)(C), 15 U.S.C. § 7001(c)(1)(C).

167. *Id*. § 101(c)(1), 15 U.S.C. § 7001(c)(1).

to be *delivered* to the consumer. In short, Subsection (c) refers to a consumer protection statute that contains a copy-delivery requirement.

To understand this issue it is necessary to discuss the basic types of consumer protection statutes. There are three:

> ??Type (i), Copy Delivery Requirement. This kind of statute requires delivery of a copy of information. An example is the closed-end credit disclosure required under Regulation Z requiring that disclosure be made "in writing, *in a form that the consumer may keep*."[168]
>
> ??Type (ii), Disclosure Only, Any Method. This kind of statute requires that disclosures be made but does not specify the method for making them. The disclosing party may choose any method, including oral disclosure that cannot be seen, or written disclosures that can be seen (on paper or electronically) but not necessarily retained.[169]
>
> ??Type (iii), Written Disclosure But No Copy Delivery Requirement. This type of statute falls into the middle of the first two categories. Under this type, a writing is required but there is no requirement to provide a copy to the consumer and the "writing" requirement can be met with anything that produces visual text—to wit, metal signs on cash registers or painted notices on walls.[170] An example of Type (iii) is provided by the federal Magnuson-Moss Warranty Act.[171] By definition, the act only applies to warranties that are written.[172] For

168. Regulation Z, 12 C.F.R. § 226.17(a) (2001) (emphasis added).

169. *See, e.g.*, FTC Telemarketing Sales Rule, 16 C.F.R. §310.3(a)(1) (2001) (requiring disclosure of certain items before a customer pays for goods or services, but not requiring the disclosure to be in a writing or other record). The staff introduction to this aspect of the rule notes that "[t]hese disclosures may be made either orally or in writing." Telemarketing Sales Rule, 60 Fed. Reg. 43,846 (Aug. 23, 1995) (to be codified at 16 C.F.R. pt. 310).

170. *See, e.g.*, *In re* RealNetworks Privacy Litig., No. 00C 1366, 2000 WL 631341, at *3–4 (N.D. Ill May 8, 2000). The court found that the writing requirement in an arbitration act can be met with electronic characters:

> Although the definition of a writing included a traditional paper document, it did not exclude representations of language on other media. Because electronic communications can be letters or characters formed on the screen to record or communicate ideas be [sic] visible signs and can be legible characters that represent words and letters as well as form the conveyance of meaning, it would seem that the plain meaning of the word "written" does not exclude all electronic communications. That being said, the Court does not now find that all electronic communications may be considered "written".

Id. at *3.

171. 50 U.S.C. §§ 2301–2312 (1994).

172. *Id.* § 2302(a) (placing requirements on "any warrantor warranting a consumer

> written warranties, retailers must make the text of the warranty available for examination by the prospective buyer.[173] This is typically done with paper notebooks of warranty terms that the retailer maintains and lends to the consumer for review. The retailer is *not* required to purchase a photocopy machine or retain the personnel necessary to print copies for the consumer. The consumer looks at the written text and then returns the notebook.

Clearly, Subsection (c) *applies* to the Type (i) statutes. It does *not* apply to Type (ii) because they do not require a writing.

As to Type (iii), E-Sign should not apply. E-Sign preserves existing law except as to writing and signature requirements:

> (b) PRESERVATION OF RIGHTS AND OBLIGATIONS—This title does not—
>
> (1) limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form . . . .[174]

Interpreting Subsection (c) to apply to Type (iii) statutes would change underlying law and create imbalances between electronic and non-electronic commerce. This is illustrated by the following example:

> ??Retailer #1 supplies notebooks containing manufacturer warranty terms to comply with the Magnuson-Moss Warranty Act. When replacements are received from manufacturers, the retail staff updates the notebooks when employees can get to it. Thus, different branches of the retailer update at different times and some papers are lost even though commercially reasonable efforts are used.
>
> ??Retailer #2 builds a computer network and hires programmers to create and maintain a database out of the warranty terms supplied by manufacturers and places a computer in every retail branch. Whenever an update is entered into the database, it is available immediately at all branches.

Retailer #2 provides the greatest benefit to consumers. But must

---

product to a consumer by means of a written warranty").

173. 16 C.F.R. § 702.3(a) (2001).

174. E-Sign § 101(b)(1), 15 U.S.C. § 7001(b)(1) (2000).

it also comply with Subsection (c), and must it maintain a notebook system in *addition*, in case one consumer says that he would rather look at a notebook? The answer should be no. The Magnuson-Moss Warranty Act simply requires that written terms be made available for review. It does not limit the ways in which that review can be accomplished. Furthermore, it does not contain a copy delivery requirement.[175] Each retailer made the written warranty terms available for review, and that is enough. If Subsection (c) is construed as applying to Type (iii) statutes, then Retailer #2 is not in compliance because it does not supply an E-Sign Disclosure Statement to each consumer before providing the warranty terms electronically. How could it do so? Many of the required disclosures could not even be answered accurately, usefully, or with any sense. Consider this attempt:

> E-SIGN DISCLOSURE STATEMENT
>
> You have no right or option to have the warranty terms to be made available on paper. *[True, but why make the statement? Magnuson-Moss only requires that written warranty terms be made available for review before purchase–it does not require delivery of a paper copy.]*
>
> If you consent to receiving the terms electronically, you may withdraw that consent if you _____ but the consequences will be _____. *[Nonsensical–the consumer's consent is not required at all unless E-Sign amends the Magnuson-Moss Warranty Act and creates a discrimination between Retailers #1 and #2.]*
>
> The hardware and software necessary for access to and retention of the warranty terms are _____. [*How to answer this? The consumer does not need any hardware or software for access; it is all supplied by the retailer at the store, and it is irrelevant what kind it is or whether the consumer's home system is compatible. As for retention, the retailer is not required to provide a copy. If the consumer decides to buy the product, the copy is supplied with the product.]*
>
> You may obtain a paper copy of the warranty terms by _____. *[There is no accurate answer. The consumer is not entitled to obtain a paper copy at all. The retailer provides notebooks for review, not copies to take home.]*

Also note that the "electronic handshake" rule in subsection (c)(1)(C) (discussed below) cannot be met at all by Retailer #2

175. *See generally* Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, 50 U.S.C. §§ 2301–2312 (lacking any copy delivery requirement).

unless congressional statements can be relied upon.[176] The consent the consumer must give *if* Subsection (c) were applied to Type (iii) statutes (the consent that Magnuson-Moss does not require for paper notebooks), must be given *electronically* to prove the consumer has the necessary software and hardware to receive the Consumer Protection Disclosure Statement. But, in the hypothetical, all of the software and hardware is the retailer's and the consumer never needs her own software and hardware. Thus, the electronic consent requirement cannot be met or means nothing. In fact, the drafters of E-Sign acknowledge this. The materials quoted in Part IV.C below make it clear that the drafters had in mind an e-mail or Web-based handshake between two different computer systems—the retailer's and the one that will be used by the consumer. While actual access might satisfy the handshake requirement and therefore moot this issue, disclosure requirements are not drafted to accommodate that.[177]

The point is that Subsection (c) is not designed to apply to Type (iii) consumer protection statutes and E-Sign itself was not intended to disturb underlying law. Again, this previously quoted statement from Senator Abraham is helpful:

> Section 101(c) honors the provisions of underlying law (except as to the specifics of writing and consent requirements*); the Act does not create new requirements for electronic commerce* but simply allows disclosures or other items to be *delivered* electronically instead of on paper. This means *that if a consumer protection statute requires delivery of a paper copy of a disclosure or item to a consumer,* then the consent and disclosure requirements of subsection (c)(1)(A-D) must be satisfied. *Otherwise, subsection (c) does not disturb existing law*.[178]

Questions may arise, however, about underlying law. For example, even before E-Sign was adopted, the FTC acknowledged that retailers subject to Magnusson-Moss rules have the choice to supply warranty terms electronically or non-electronically. It did so by assuming, without case law, that a warranty offered online

176. Refer to Part IV.C *infra* (discussing how Sens. Abraham and McCain emphasized both that the statute's reasonable demonstration requirement is not intended to burden consumers or persons providing the electronic record, and that the requirement may be satisfied in many ways).

177. *See generally* E-Sign § 101, 15 U.S.C. § 7001 (lacking both a requirement that a consumer have actual access to disclosures and a specific allowance by which actual access would satisfy the statute).

178. Abraham Statement of June 16, 2000, *supra* note 36, at S5284 (emphasis added).

triggers the Magnuson-Moss Warranty Act,[179] which literally only applies to "written" warranties.[180] Putting that aside, the FTC unquestionably went beyond the federal warranty act with the following suggestion that the text must not only be made available, but must be in a form that the consumer may download or print:

> Because consumers may need to refer to the warranty while comparison shopping or after the purchase, the warranty should be presented in a way that is capable of being preserved, either by downloading or printing. This is especially important if a paper warranty is not included with the product.[181]

While that is fine as a suggestion for a good—but not legally required—business practice, any mandate to provide a copy is without statutory basis and would prevent some electronic transactions. It will also create discrimination between electronic and non-electronic commerce or create significant new costs. For example, if a consumer were surfing the Web on a hotel television, there would be no ability to download or print the warranty text displayed. However, the retailer will still have complied with the federal warranty act by displaying the text in writing, and the consumer will still have available the ability to see warranty text while shopping. This is no different than in physical stores where the store complies with the federal warranty act by making the notebooks available for review—but that store is not *also* required to provide a copy that the consumer may retain. By inventing such a requirement, the FTC not only exceeds its statutory authority but discriminates between electronic and non-electronic commerce.

C. The Electronic Handshake Rule.

Under E-Sign subsection (c), the requirement to provide a Consumer Protection Statute Disclosure Statement in writing is satisfied if the consumer "*consents electronically, or confirms* his

---

179. The Federal Trade Commission stated that:

> [s]ellers that offer written warranties on consumer products must include certain information in their warranties and make them available for review at the point of purchase. Warranties communicated through visual text on Web sites are no different than paper versions and the same rules apply. . . .

Federal Trade Commission, Dot Com Disclosures, at section IV(A)(2), *available at* http://ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.html.

180. Magnuson-Moss Warranty–Federal Trade Commission Improvement Act, 50 U.S.C. §§ 2302(a), 2303(a) (limiting the statute's reach to written warranties).

181. Federal Trade Commission, Dot Com Disclosures, at section IV(A)(2), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/dotcom/index.html.

or her consent *electronically,*[182] *in a manner that reasonably demonstrates that* the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent."[183] The focus of the discussion in this section is on the *method* for consent—that is, what is called an "electronic handshake."

Subsection (c) requires that the consumer affirmatively consent to receipt of the Consumer Protection Statute Disclosure Statement after receiving the E-Sign Disclosure Statement.[184] Under the "reasonable demonstration" requirement, referenced herein as an "electronic handshake," the consumer must provide, or confirm, her consent *electronically* in a manner that reasonably demonstrates she will be able to access the Consumer Protection Statute Disclosure Statement once it is sent to her.[185]

One senator explained the electronic handshake as follows:

> Most importantly, the consumer must consent electronically or confirm his or her consent electronically in a manner that reasonably demonstrates that the consumer can access the information in the electronic form that will be used to provide the information. This is critical. "*Reasonably demonstrates" means just that. It means the consumer can prove his or her ability to access the electronic information that will be provided. It means the consumer, in response to an electronic vendor enquiry, actually opens an attached document sent electronically by the vendor and confirms that ability in an e-mail response.*
>
> It means there is a two-way street. It is not sufficient for the vendor to tell the consumer what type of computer or software he or she needs. It is not sufficient for the consumer merely to tell the vendor in an e-mail that he or she can access the information in the specified formats. There must be meaningful two-way communication electronically between the vendor and consumer.[186]

More senators disagreed with this characterization of the electronic handshake rule. This is likely because the above characterization forces the disclosing party to assume the

182. Note that this is an *affirmative* consent to the substitution of an electronic Consumer Protection Statute Disclosure Statement. It is not an "opt out" structure in which an electronic Consumer Protection Statute Disclosure Statement could be delivered unless the consumer says otherwise.

183. E-Sign § 101(c)(1)(C)(ii), 15 U.S.C. § 7001(c)(1)(C)(ii) (2000) (emphasis added).

184. *Id*. § 101(c)(1), 15 U.S.C. § 7001(c)(1).

185. *Id*. § 101(c)(1)(C), 15 U.S.C. § 7001(c)(1)(C).

186. 146 CONG. REC. S5216 (daily ed. June 15, 2000) (statement of Sen. Wyden) (emphasis added).

customer is lying, and that assumption is not typically built into U.S. law. As an example, the following explanations were submitted by Senator Abraham:

> . . .The requirement of a reasonable demonstration is not intended to be burdensome on consumers or the person providing the electronic record, and *could be accomplished in many ways. For example, the 'reasonable demonstration' requirement is satisfied if the provider of the electronic records sent the consumer an e-mail with attachments in the formats to be used in providing the records, asked the consumer to open the attachments in order to confirm that he could access the documents, and requested the consumer to indicate in an e-mailed response to the provider of the electronic records that he or she can access information in the attachments.* Similarly, the 'reasonable demonstration' requirement is satisfied if it is shown that in response to such an e-mail the consumer actually accesses records in the relevant electronic format. The purpose of the reasonable demonstration provision is to provide consumers with a simple and efficient mechanism to substantiate their ability to access the electronic information that will be provided to them.[187]

Senator Abraham had previously stated the following:

> Under the consent provisions, a consumer must affirmatively consent to the provision of records in electronic form, and there must be a reasonable demonstration that the consumer can access electronic records. *For the immediate future, the conference envisions this "electronic consent" to take the form of either a Web-page based consumer affirmation, or a reply to a business' electronic mailing which includes an affirmation by the consumer that he or she could open provided attachments.* I eagerly await future technology developments that render the burdens this section imposes on consumers and businesses obsolete.[188]

In addition, the following "floor" exchange between Senators McCain and Abraham exemplifies the latitude intended under the electronic handshake rule:

> Mr. McCAIN. Is it the Senator's understanding that pursuant to subsection 101(c)(1)(C)(ii) of the conference report a consumer's affirmative consent to the receipt of

187. Abraham Statement of June 16, 2000, *supra* note 36, at S5284 (emphasis added).

188. 146 CONG. REC. S 5224 (daily ed. June 15, 2000) (statement of Sen. Abraham) (emphasis added).

> electronic records needs to "reasonably demonstrate" that the consumer will be able to access the various forms of electronic records to which the consent applies?
>
> Mr. ABRAHAM. Yes. The conference report requires a "reasonable demonstration" that the consumer will be able to access the electronic records to which the consent applies. *By means of this provision, the conferees sought to provide consumers with a simple and efficient mechanism to substantiate their ability to access the electronic information that will be provided to them.*
>
> Mr. McCAIN. I agree. *The conferees did not intend that the "reasonable demonstration" requirement would burden either consumers or the person providing the electronic record. In fact, the conferees expect that a "reasonable demonstration" could be satisfied in many ways. Does the Senator agree with me that the conferees intend that the reasonable demonstration requirement is satisfied if the consumer confirmed in an e-mail response to the provider of the electronic records that he or she can access information in the specified formats?*
>
> Mr. ABRAHAM. *Yes.* An e-mail response from a consumer that confirmed that the consumer can access electronic records in the specified formats would satisfy the "reasonable demonstration" requirement.
>
> Mr. McCAIN. *Does the Senator also agree with me that the "reasonable demonstration" requirement would be satisfied, for instance, if the consumer responds affirmatively to an electronic query asking if he or she can access the electronic information or if the affirmative consent language includes the consumer's acknowledgement that he or she can access the electronic information in the designated format?*
>
> Mr. ABRAHAM. *Yes.* A consumer's acknowledgment or affirmative response to such a query would satisfy the "reasonable demonstration" requirement.
>
> Mr. McCAIN. *Would the "reasonable demonstration requirement" be satisfied if it is shown that the consumer actually accesses records in the relevant electronic format?*
>
> Mr. ABRAHAM. *Yes.* The requirement is satisfied if it is shown that the consumer actually accesses electronic records in the relevant format.[189]

189. 146 CONG. REC. S 5282 (daily ed. June 16, 2000) (statements of Sens. McCain and Abraham) (emphasis added).

Courts will ultimately determine what is reasonable, and it would be unusual in U.S. law to force vendors to assume that their customers are lying. If that is correct (that the vendor may believe the customer), then it would seem that the electronic handshake rule can be met in many ways, including reliance on an e-mail statement of the consumer or by adopting a self-proving method. If the consumer states in an e-mail that he is able to access the format to be used by the Consumer Protection Statute Disclosure Statement, or if the consumer consents or confirms consent in the same electronic manner that is or will be used to provide the Consumer Protection Statute Disclosure Statement, then it should be reasonable to assume that the consumer will be able to receive and open that disclosure once it is delivered.

With respect to all of Subsection (c), what does it really mean? Judicial interpretation may be necessary but, hopefully, it will be consistent with this Article and the "legislative history" of E-Sign. This Article interprets Subsection (c) in light of its commendable purposes of enabling e-commerce while at the same time providing reasonable protection to consumers who prefer to continue to receive—on paper—consumer protection disclosures and notices that currently must be delivered on paper. This interpretation also avoids discrimination against e-commerce and unannounced substantive changes in existing contract and consumer protection laws.

V. LOOKING AT "E-SIGNATURE" LEGISLATION, WHAT KINDS OF MISTAKES ARE BEING MADE?

Several mistakes are being made in e-signature or e-commerce legislation. While some appear to be small mistakes, any mistake tends to have unintended consequences. This has the potential to distort or disturb substantive law that was not intended to be changed or that should not have been changed. Thus, it is helpful to examine sample mistakes and, hopefully, avoid or repeal them in the future. Here are some examples:

A. Mistake #1: Making Erroneous Assumptions That Create Harmful Disparities Between Electronic and Non-Electronic Commerce

One example of this mistake can be seen in electronic commerce legislation imposing record, timing, or delivery requirements that would not exist but for erroneous assumptions about "writing" requirements. Section 8(a) of UETA, for example, states:

> If parties have agreed to conduct a transaction by electronic means and a law requires a person to provide, send, or deliver information in *writing* to another person, the requirement is satisfied *if* the information is provided, sent, or delivered, as the case may be, in an electronic record capable of *retention* by the recipient *at the time of receipt*.[190]

This provision may assume that every "writing" requirement is a requirement for delivery of a copy, which of course is not the case.[191] If inappropriately interpreted, this provision may also assume that every "copy delivery" requirement is a requirement for delivery at the time information is provided. Again, that may or may not be true under UETA and clearly it is not true under E-Sign.[192] Both of these interpretations of UETA may be, and hopefully are, wrong. The point is that the legislation creates an ambiguity that did not need to be created.

To illustrate, assume a traveling commercial customer uses a "mouse" supplied with the television set in his hotel room to place an order for an Internet product. Also assume that applicable law requires the vendor's refund policy to be provided "in writing" and the screen displays the policy before the "order now" button can be activated. At the vendor's offline outlets, the policy is taped to all cash registers or painted in large letters on the wall behind the register. At the time the required disclosure is made in writing on the screen, there is no capacity to provide a copy because there is no printer in the hotel room while, in the offline store, the vendor has no copy machine, has never supplied a copy, and has been in compliance with the law for many years.

Has the refund disclosure statute been violated? If the answer is "no" under the refund statute but "yes" under UETA, then UETA imposes burdens on e-commerce that do not exist in non-electronic commerce. UETA does not apply to transactions in the physical store, so it is only the online display that is affected. If the provision is read to require the online store to (1) deliver a copy at all, or (2) deliver it at the time the information is provided on screen, then UETA's provisions are discriminatory and change underlying law substantively, even though UETA purports not to make such changes and, constitutionally, likely could not do so without more.

What are other or clearer approaches? UETA speaks in

190. UETA § 8(a) (1999).

191. Refer to Part IV.B.4.iii *supra* (discussing Type (iii) statutes, which require written disclosure but no copy delivery).

192. Refer to Part IV.B.4.iii *supra* (discussing E-Sign in the context of Type (iii) statutes).

terms of a record that is *capable* of retention by the recipient *at the time of receipt*. In E-Sign Section 101(e), new requirements are imposed where a law requires that a contract or record be in "writing." In such cases, E-Sign creates equivalency by stating that an electronic record can suffice, but also states that the electronic record must be "capable of being retained and accurately reproduced" for later reference by all persons entitled to retain such.[193] While one can criticize this provision for creating rules for electronic records that do not exist for paper records, the E-Sign wording nevertheless avoids the timing mistake made in UETA by omitting some of the UETA language. The following comments by the primary drafter makes it clear that this was intentional:

> With respect to Section 101(e), *the actual inability of a party to reproduce a record at a particular point in time does not invoke this subsection*. The subsection merely requires that if a statute requires a contract to be in writing, then the contract should be capable of being retained and accurately reproduced for later reference by those entitled to retain it. Thus if a customer enters into an electronic contract which was capable of being retained or reproduced, but the customer chooses to use a device such as a Palm Pilot or cellular phone that does not have a printer or a disk drive allowing the customer to make a copy of the contract at that particular time, this section is not invoked. *The record was in a form that was capable of being retained and reproduced by the customer had it chosen to use a device allowing retention and reproduction*.[194]

In fact, the ambiguity in UETA's unfortunate wording can be resolved by interpreting it per the E-Sign clarification. As noted, UETA speaks in terms of a record that is *capable* of retention by the recipient *at the time of receipt*—in the example the record is capable of retention at that time, even though the consumer chose to use a device that made her incapable of taking advantage of the capability at that particular time. That does not mean that the provider of the writing did not meet the capability requirement.

B. Mistake #2: Unnecessarily Twisting Contract Law

Again, UETA provides an example. In section 5, UETA

193. E-Sign § 101(e), 15 U.S.C. § 7001(e) (2000).

194. Abraham Statement of June 16, 2000, *supra* note 36, at S5284 (emphasis added).

states that its e-commerce provisions do not apply unless the parties have "agreed to conduct transactions by electronic means."[195] It is perfectly appropriate to make it clear that parties are not forced to engage in e-commerce. E-Sign makes that point in section 101(b)(2) by providing simply that E-Sign does not require any person—other than certain governmental agencies—to agree to use or accept electronic records or electronic signatures.[196] UCITA has a similar provision.[197]

But UETA goes further by requiring an "agreement" to engage in e-commerce, and then compounds this problem by prohibiting parties from varying that rule by contract.[198] The official comments to UETA attempt to rectify this error by making it clear that a real agreement is not really intended. Comment 4 explains that if I hand you my business card with my email address on it, I have "agreed" to communicate electronically for business purposes as long as the communications are not "outside the scope of the business indicated by use of the card."[199] That is legally wrong and inadvisable in any case. I have given you contact information but I have not "agreed" to do anything simply by handing you my card. I am free, without breach of an "agreement," to refuse to make contracts or deal with you by phone, email, or fax even though all of that information is on my card. If, because of UETA, I am not free to make those refusals, then the UETA provision is an example of Mistake #1.[200]

This is not to say that conduct, such as handing someone a business card, cannot form an agreement.[201] The defect in the

195. UETA § 5(b).

196. E-Sign § 101(b)(2), 15 U.S.C. § 7001(b)(2).

197. UCITA § 107(b) (2000) ("This Act does not require that a record or authentication be generated, stored, sent, received, or otherwise processed by electronic means or in electronic form.").

198. UETA § 5(c) ("The right granted by this subsection [to conduct a transaction by electronic means] may not be waived by agreement.").

199. *Id*. § 5 cmt. 4(B).

200. Refer to Part V.A *supra* (discussing assumptions that create harmful disparities between electronic and non-electronic commerce).

201. *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 19 (1979). Section 19 provides:

> (1) The manifestation of assent may be made wholly or partly by written or spoken words or by other acts or by failure to act.
>
> (2) The conduct of a party is not effective as a manifestation of his assent unless he intends to engage in the conduct and knows or has reason to know that the other party may infer from his conduct that he assents.
>
> (3) The conduct of a party may manifest assent even though he does not in fact assent. In such cases a resulting contract may be voidable because of fraud, duress, mistake, or other invalidating cause.

UETA comment is the assumption that the act of handing over the card is automatically intended to be an agreement. Typically, for conduct to count as agreement, it must be done with reason to know that the other party may infer assent from the conduct—such as clicking on a "submit" button after being informed that the click will constitute agreement to stated terms.[202] By drafting the "agreement" requirement into UETA, the drafters created a problem that they then tried to solve with a comment that is not consistent with contract law. The better approach is that used by UCITA and E-Sign—that is, simply stating that nothing in those acts requires persons to deal electronically.[203]

C. Mistake #3: Freezing Laws Written for an Old Era Even Though They Will be Used in a New Era

This is a subtle error that can be seen by comparing E-Sign section 101(b)(1) with UETA section 8(b). Both statutes laudably attempt to protect the substance of existing law while enabling e-commerce. Assume a consumer statute requiring that a disclosure be made in 1 inch red letters on a white background. E-Sign preserves such requirements by stating that nothing in E-Sign alters them,[204] while UETA tries to do the same thing but

---

Id. *See also* UCITA § 112 (defining manifestation of assent and opportunity to review).

202. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000). In *Register.com*, an Internet domain name registrar sought a preliminary injunction against Verio, who used registration information for direct marketing purposes. *Id*. at 241. The Internet domain name registrar was required by contract with the Internet Corporation for Assigned Names and Numbers (ICANN) to maintain a database of registration information and permit its use for any lawful purpose subject to two exceptions, one of which required the registrar to prohibit use of the data for unsolicited commercial solicitations. *Id*. at 242. Registrar.com included all prohibitions in its terms of use, and all queries of the data base could only be made after seeing this phrase: "[b]y submitting this query, you agree to abide by these terms." *Id*. at 243. Verio claimed although it was aware of the terms of use, it was not bound by them because it had not clicked on an icon, it had instead merely submitted the query. *Id*. at 248. The court disagreed:

> The conclusion of the terms paragraph states "[b]y submitting this query, you agree to abide by these terms." Verio does not argue that it was unaware of these terms, only that it was not asked to click on an icon indicating that it accepted the terms. However, in light of this sentence at the end of Register.com's terms of use, there can be no question that *by proceeding to submit a WHOIS query, Verio manifested its assent to be bound* by Register.com's terms of use, *and a contract was formed* and subsequently breached.

Id. (alteration in original) (citations omitted) (emphasis added). *See also, e.g.*, M.A. Mortenson Co. v. Timberline Software Corp., 970 P.2d 803, 809 (Wash. Ct. App. 1999), *aff'd*, 998 P.2d 305 (Wash. 2000) ("We find that Mortenson's installation and use of the software manifested its assent to the terms of the license and that it is bound by all terms of that license that are not found to be illegal or unconscionable.").

203. *See* E-Sign § 101(b)(2), 15 U.S.C. § 7001(b)(2) (2000); UCITA § 107(b).

204. *See* E-Sign § 101(b)(1), 15 U.S.C. § 7001(b)(1) (preserving the rights and

says it in a way that creates problems. UETA expressly states that if another law contains such requirements, then those requirements must be met in the manner specified in the other law.[205] One reading of UETA is that it may prevent courts from construing old statutes to meet new circumstances.

To illustrate this problem, note that under existing law a court could take one of two approaches in interpreting the "1 inch, red letters on white" requirement in a fifty year old statute. It could either require strict compliance, or conclude that the purpose of the statute was to make conspicuous the relevant text. Assume a party claims violation of the statute because they used a hand-held device that only allowed 3/4 inch red letters on a gray background. Further assume that white is not possible (at any practical cost that would allow use by a consumer) to produce on the device. If a court were convinced that the notice intended by the statute had been given—even though its literal terms were not met—it could enforce the notice in order to accommodate changes in commerce and the practical inability of jurisdictions to amend every single statute. The question is whether UETA allows or prohibits such a decision. If the answer is that it "prohibits," then that is a mistake. It would also be a mistake to advocate that e-commerce vendors are free to ignore such statutes. The question is whether courts will be given any leeway to re-interpret their literal terms or purpose within judicial boundaries. Those boundaries could themselves preclude the hypothesized decision, but new e-commerce legislation should not preclude it.

E-Sign expressly preempts one UETA problem of this type. Section 8(b)(2) of UETA provides that if a law requires a record to be delivered in a particular manner, then an electronic record must be delivered in the same manner.[206] Official Comment 4 to UETA gives an example of a statute requiring that a notice be sent by first-class mail. In such a circumstance, UETA requires an electronic notice to be placed on a disc and then mailed! Not surprisingly, E-Sign didn't buy that. E-Sign section 102(c) provides that even states adopting a "pure" UETA to otherwise escape federal preemption may not circumvent E-Sign through

obligations set by other statutes, regulations, and rules of law).

205. UETA § 8(d) (1999) ("[T]o the extent a law other than this [Act] requires information to be provided, sent, or delivered in writing but permits that requirement to be varied by agreement, the requirement . . . that the information be in the form of an electronic record capable of retention may also be varied by agreement.") (alteration in original).

206. *Id*. § 8(b)(2) ("The record must be sent, communicated, or transmitted by the method specified in the other law.").

"the imposition of nonelectronic delivery methods under section 8(b)(2)" of UETA.[207] E-Sign section 102(a)(1)[208] also restricts how states can exercise their rights under section 3(b)(4) of UETA (which allows states to exclude certain laws from UETA). Senator Abraham explained the policy in the following statement:

> . . .UETA includes a provision that permits a state to prescribe "delivery methods" for various records. I saw this as a potential loophole to the bill, which would allow a state to circumvent the intent of the general rule and require that an electronic document be delivered via physical methods—most likely "first class" mail. *It should be clear to all that the federal legislation would not permit such a delivery method requirement, and we have specified as much in the preemption section*.[209]

> Subsection (a)(1) [of E-Sign Section 102] places a limitation on a State that attempts to avoid Federal preemption by enacting or adopting a clean UETA. Section 3(b)(4) of UETA, as reported and recommended for enactment by NCCUSL, allows a State to exclude the application of that State's enactment or adoption of UETA for any 'other laws, if any, identified by State.' This provision provides a potential loophole for a State to prevent the use or acceptance of electronic signatures or electronic records in that State. To remedy this, subsection (a)(1) requires that any exception utilized by a State under section 3(b)(4) of UETA shall be preempted if it is inconsistent with title I or II, or would not be permitted under subsection (a)(2)(ii) (technology neutrality). Requirements for certified mail or return receipt would not be inconsistent with title I or II, *however, note that an electronic equivalent would be permitted*.[210]

D. Mistake #4: Assuming That Signatures Must Identify the Person Signing

An example of this kind of mistake can be seen in the revised version of U.C.C. Article 9 and in proposed commentary to a

207. E-Sign § 102(c), 15 U.S.C. § 7002(c).

208. *Id.* § 102(a)(1), 15 U.S.C. § 7002(a)(1) (making the exception that a state statute enacting UETA may modify or supercede the provisions of E-Sign "except that any exception to the scope of such Act . . . shall be pre-empted to the extent such exception is inconsistent with this title or title II").

209. 146 CONG. REC. S5224 (daily ed. June 15, 2000) (statement of Sen. Abraham) (emphasis added).

210. Abraham Statement of June 16, 2000, *supra* note 36, at S5285 (emphasis added).

Federal Reserve Board Regulation.[211] The Article 9 definition of "authenticate," which is the term that the U.C.C. and UCITA use in place of "signature" (both electronic and non-electronic), requires the authenticating party (the signer) to execute a symbol with the intent to "identify" herself and accept the record being signed.[212] The problem, of course, is that not all signatures "identify" a person—an "X" is sufficient to sign a will even though it might not actually identify anyone. More important are statutes that require a signature and then trigger legal consequences regardless of whether the signature identifies the signing party. For example, under Article 3 (Negotiable Instruments) of the U.C.C., an "order" must be "signed," and a negotiable instrument is an order or unconditional promise to pay a fixed amount of money that meets certain other requirements.[213] If a negotiable instrument is forged on paper, there is a signature of the forger, and the document is a negotiable instrument even though it is forged. The forger, as the signing party, is liable to pay the instrument—if he or she can be found—but the signature does *not* identify the forger. To the contrary, it identifies the person who is not liable on the instrument, the victim of the forgery. A different rule should not be created for e-commerce. Traditional signatures do not always identify the signing party, and any other rule for e-signatures will have unintended consequences.

E. Mistake #5: Altering Traditional Definitions by Inaccurately Summarizing or Unnecessarily Limiting Them

U.C.C. Revised Article 9-102(7)(B) provides an example of this problem. It defines "authenticate" (the new U.C.C. and UCITA term for "sign") as follows: "[t]o execute or otherwise adopt a symbol, or encrypt or similarly process a record in whole or in part, with the present *intent* of the authenticating person *to* identify the person and *adopt or accept a record*."[214] Compare this formulation with U.C.C. Article 1-201(39), which defines "signed" as including "any symbol executed or adopted by a party with present *intention to authenticate* a writing."[215] The Article 1 formulation for "signed" is carried into E-Sign, UETA, and UCITA in terms of adopting a symbol with the *intent to sign* the

211. Refer to note 62 *supra* (arguing that FRB Staff commentary for a proposed regulation interpreting E-Sign adds, without authority, an identity requirement).

212. U.C.C. § 9-102(7) (Revised 2001).

213. *Id*. § 3-103(a)(6) (2000).

214. *Id*. § 9-102(a)(7).

215. *Id*. § 1-201(39) (2000) (emphasis added).

record.[216] In other words, each of those statutes carries forward the traditional definition of "sign," whatever it may be, and then updates it. But the statutes do not try to summarize the meaning of sign or to alter it (except for updating it for e-commerce). E-Sign, UETA, and UCITA took this approach because it is not really possible to set forth all possible meanings of "sign."

Revised Article 9 provides a sharp contrast. Its definition contemplates that a signature may only do one thing—that is, evidence an intent to "adopt or accept" a record. In contrast, traditional signatures may do eight or more things. A good list, but not necessarily complete, appears below. Note that the many listed functions of a signature include much more than is contemplated by the Revised Article 9 definition:

> *Identification*. The addressee can verify the signer's identity by checking the signature.
>
> *Authentication*: the signature authenticates the declaration, which is included in the writing concerned. The writing reflects the facts correctly, unless evidence to the contrary is produced.
>
> *Declaration of will*. By signing the signer manifest his will and declares to be legally bound to the intention included in the writing concerned.
>
> *Authorization*. The signer implicitly declares being authorized to perform a legal act, for example, in case of representation.
>
> *Safeguard against undue haste*. By putting one's signature to a document, the signer is notified that legal consequences may be involved. Thus, the signer is protected against undue haste.
>
> *Non-repudiation of origin or receipt*. The signer cannot deny that she has sent or received a document, unless proven otherwise.
>
> *Notice of contents*. The signer implicitly indicates that she knows the contents of the document.
>
> *Integrity*. Putting one's signature at the end of the document guarantees, to some extent, that the document has not been altered afterwards, thus, reducing the possibility of fraudulent actions.
>
> *Originality*. Signing a document distinguishes the original

216. E-Sign § 106(5), 15 U.S.C. § 7006(5) (2000); UCITA § 102(a)(6) (1999); UETA § 2(8) (1999).

from a copy.[217]

Properly written, Article 9 would not limit its definition of authentication to adopting or accepting a record. This ignores or alters many other reasons a person may authenticate a document. The justification offered by Article 9 representatives, when asked about this during the drafting process, was that Revised Article 9 only speaks of authentication in those terms and no other terms. That, however, is a questionable conclusion. For example, revised U.C.C. Article 9-104, regarding control agreements, contemplates that a bank will give a secured creditor an authenticated record indicating that the bank will comply with the secured creditor's instructions.[218] Under section 208, a secured creditor who has control of a deposit account must, upon receipt of an authenticated demand from the debtor, give an authenticated statement to the bank releasing control of the account.[219] In each case, it would likely be more accurate to view the authenticated record requirement as implementing the "non-repudiation of origin or receipt" function of a signature, that is, the requirement ensures that the signer cannot deny that he has sent or received a document, unless proven otherwise. That is, or may be, different than "adopting or accepting" the record, yet that is the definition of authentication in Revised Article 9.

VI. CONCLUSION

Many issues arise in e-signature legislation, and the U.S. approach is only one of them. The purpose of this Article has been to explain, for the consideration of those interested in the U.S. approach, some of its basic rules for electronic signatures and to illustrate the need for extreme care when drafting e-commerce legislation. Only time and case law will supply actual guidance, and this Article has assumed that E-Sign, in fact, will be construed to accomplish its purpose. That purpose is to

217. Refer to note 15 *supra* and accompanying text (discussing various functions of signatures in Dutch legislation). The study that produced this list is referenced in a subsequent Dutch study and report. AALBERTS & VAN DER HOF, *supra* note 15, § 4.3.1.1.

218. U.C.C. § 9-104(a)(2).

219. *Id.* § 9-208(b)(1) (providing a maximum of ten days for the secured party to release the bank from further obligation).

establish equivalency between electronic and non-electronic commerce while not upsetting traditional substantive contract law or practices. E-Sign is an important act and is welcomed as a uniform guidepost in the information economy.

APPENDIX 1

FEDERAL E-SIGN AND UETA: PROPOSED STATE BAR REPORT AND RECOMMENDATION

Jeff Dodd

I. BASIC PREMISE: ELECTRONIC VALIDATION ALREADY EXISTS

The basic premise in this discussion is that enactment of federal legislation affects how Texas should proceed with reference to state legislation relating to electronic signatures and records. Enactment of the federal Electronic Signatures in Global Commerce Act (Federal Act) altered Texas law to provide for the adequacy of electronic records and signatures in ordinary commerce, and to provide somewhat different rules for the treatment of electronic records in reference to required consumer disclosures. That result occurred by virtue of the preemptive effect of the Federal Act.

Because the Federal Act represents current law, consideration of *further* action as a matter of state law must be viewed as exactly that: consideration of whether Texas should take further action with respect to validating electronic records and signatures. In order to justify recommending that Texas do so, we must conclude that further action creates benefits that justify both the effort and that off-set any negative effects that further action might have in reference to the certainty, national uniformity and workability of rules on electronic commerce with respect to validation of electronic records and signatures.

More specifically, in addition to other issues, we should consider the following:

?? Are there benefits that can ensue from displacing existing Federal Act rules with state law and what are those benefits?

?? On balance, are rules contained in our available state legislative options superior or equivalent to current law in light of the Federal Act?

?? What course of action will better serve uniformity in electronic validation or adequacy rules between Texas law and law on a national basis?

To repeat, however, the baseline for this decision assumes that current law in Texas reflects the Federal Act. It is **not** necessary to take further action to establish that electronics are generally equivalent to writings.

II. OPTIONS CONSIDERED AND RECOMMENDATION.

There may be various discrete state law actions that might improve current law and might be considered later. Our focus is on more large-scale change. There are four alternatives:

1. Recommend adoption of the uniform version of UETA to displace current law as modified by the Federal Act.

2. Recommend adoption of a modified version of UETA to displace current law as modified by the Federal Act.

3. Recommend adoption of Federal Act rules as Texas state law, to displace current law as modified by the Federal Act.

4. Recommend that no further action be taken now to modify Texas law, but perhaps that studies be undertaken to determine if particular aspects of state law may still benefit from electronic validation rules.

Based on a review of the current situation within Texas and nationally, I recommend that the State Bar propose either Alternative 3 or Alternative 4 at this time.

Alternatives 1 or 2 refer to adoption of either a modified or a pure version of UETA. Either action would be a step backward from current law and an excursion in which national uniformity of Texas and other states' law would be impossible or at least very unlikely,

On the other hand, Alternative 3 (adoption of substantive Federal Act rules as state law) would displace federal law involvement on this issue, but leave Texas in a position of national uniformity with the law of most other states in light of the Federal Act.

Alternative 4 would entail the least costly and time-consuming effort, while leaving Texas options open for the future.

III. BASIC LAW AND PREEMPTIVE EFFECT

Subject to limited subject-matter exclusions, the Federal Act precludes any state law from discriminating against electronic records or signatures solely because they are electronic. This partially preempts any state law that requires a writing, in effect replacing the state law writing requirement with a rule that would be satisfied by either a written or an electronic writing or signature.

Section 102 of the Federal Act provides that states may modify, limit or supercede federal law on this issue only in one of two ways:

?? Adoption of a pure version of UETA as promulgated by NCCUSL (Section 102(a)(1)).

?? Adoption of technologically neutral state legislation that is "consistent" with the Federal Act and that refers to the Federal Act (Section 102(a)(2)).

There are some issues about the effect of this preemption language on so-called digital signature acts present in some states, but those issues are not relevant to our current concern. As was pointed out in an article by Professor Nimmer of the University of Houston, this Federal Act "back-in" rule gives the states the ability to assert control over the electronic validation issue, but only by acting in one of two ways—enacting a pure UETA or enacting legislation "consistent" with the Federal Act rules.

A. UETA Enactment and Preemption.

The reference to displacing federal law by enacting a pure version of UETA is not qualified by any flexibility, such as a reference to a "substantially" pure UETA. Thus, as further supported in legislative comments, state enactment of a modified UETA does not qualify under section 102(a)(1) and avoids preemption only if it is "consistent" with the Federal Act.

While Congress apparently viewed UETA as a whole as a permissible alternative structure to the Federal Act rules, as pointed our below, UETA and the Federal Act are substantively different. UETA would not necessarily qualify under the reference to consistent state legislation. As a result, in holding out UETA as a possible alternative, Congress provided separately for that possibility, independent of consistency with the Federal Act.

Some argue that modified versions of UETA would not be preempted and would displace the Federal Act, except as to the differences. That interpretation is contrary to the black letter of the statute and would not likely be accepted in court. However, an even more compelling reason exists for our not adhering to that interpretation of the Federal Act: were we to do so, the actual status of Texas law would be uncertain in fact until courts definitively rule on the issue. That could take years to occur and during that time, rather than creating certainty, we would have created uncertainty and, perhaps, chaos.

B. "Consistent" State Law and Preemption.

The Federal Act allows states to displace its effect on state law by adopting *consistent* state legislation that is technologically neutral and that, if adopted after it, refers to the Federal Act.

The Federal Act does not specify what standard applies to determine whether a state law is "consistent" with the Federal Act. Thus, in most cases, use of this means to reassert state law control of electronic adequacy issues might create problems associated with uncertainty about whether a particular state rule was or was not consistent with the Federal Act. That argues against most approaches in state law to rely on this option as a basis for a global treatment of electronic adequacy questions.

However, it is quite clear that a state law that adopts rules identical to the substantive rules of the Federal Act is *consistent* with it. Why might a state such as Texas do this? One reason would be to clearly retake control of questions about the equivalence of writings and electronics, placing those issues under state court control. A second reason would be to make clear that the existing electronic adequacy rules apply both to transactions in interstate commerce and transactions that are not in that form of commerce. That is, to establish complete uniformity of law on these issues within a state and for all transactions affecting the state.

This identifies Alternative 3 as stated earlier as a viable alternative for the State Bar to propose to the Texas legislature.

C. Effect of Preemption on Alternatives.

The preemption issues argue strongly for rejecting any alternative that contemplates enactment of a modified version of UETA.

Most likely, under the literal terms of the Federal Act, such an enactment would be preempted and ineffective. It would be

considered under the standard that allows a "consistent" state law, but the substantive provisions of UETA are not consistent with the Federal Act. Even if there were some intermediate rule that preempts only the changes from the uniform UETA, one would not know whether that was true for many years, causing significant uncertainty.

Based on this, I reject and recommend that the Committee reject Alternative 2 as stated above. We are left with three choices: a pure UETA, a state enactment of the Federal Act rules, or no action to change existing law.

IV. COMPARING THE ALTERNATIVES: UNIFORMITY OF NATIONAL LAW

Which of the three remaining alternatives better serves state interests in national uniformity?

To answer this we need to clarify what are our state's interest in uniformity on the electronic adequacy issues. There are two. One is that there exists some national benefit to having a seamless, consistent web of law on the basic adequacy issue on a national basis; this benefits all U.S. commerce. The second is that Texas has an interest in not having its resident companies and individuals governed by law that is inconsistent with national standards in an area of commerce that is demonstrably national or international in nature.

Yet even with this clarification, the answer to the question is not entirely clear. The Federal Act became law in October and UETA was promulgated relatively recently. What trends will transpire nationally are unknown. Yet, on balance, it seems most likely to me that immediate enactment of a pure UETA would not serve state interests in uniformity, but would place this state in a minority position nationally. That may change in the future, but it may not. Many states are likely to conclude that current law, without UETA and based on the Federal Act, suffices.

Some have argued that enacting UETA contributes to national uniformity on the electronic validation or adequacy rule. However, that is not presently the case.

Enactment of a modified UETA would create the uncertainty about applicable law and rules alluded to above due to the potential effect of federal preemption. However, even enacting UETA in pure form would not necessarily create benefits in reference to national uniformity.

At a recent presentation, the Chair of the UETA Committee commented that, while UETA has been adopted in slightly more than twenty states, *none* of those states enacted the statute in its pure form. In this, Professor Fry was being somewhat over-

stated. Several of the enacting states changed only the numbering system in UETA and this non-substantive change clearly does not trigger preemption. However, it is true that many of the enacting states made substantive changes in the pure UETA and that, as a result, their current status under the Federal Act is highly suspect.

The basic circumstance in reference to uniformity of law are thus:

?? In a majority of all states (at least 28), the current rule is identical to the current law in Texas and is defined by the terms of the Federal Act interacting with state law requirements of a writing or a signature, when they exist.

?? In an undetermined but large number of additional states that have enacted a version of UETA, the same result prevails: the current actual law consists of the Federal Act rules interacting with local state law writing and signature requirements.

We certainly cannot safely prognosticate what will happen nationally in the wake of the Federal Act's intrusion, but it is clear that currently, only a small number of states are not governed by the federal standards interacting with state law.

Texas is exactly in that position. Its current law is a blend of the federal standards and applicable state law previously requiring writing in some transactions. To move away from that majority position is not to immediately serve uniformity interests.

This factor, thus, currently argues against Alternative 1 above (adopting a pure UETA). Instead, it favors either leaving current law in place, or adopting a state enactment of the Federal Act standards.

V. COMPARING THE ALTERNATIVES: SUBSTANTIVE BENEFITS

Ultimately, perhaps the most significant basis for choosing between current law, a state adoption of the Federal Act standards, or enactment of a pure UETA involves the substantive question of which path gives Texas the benefit of the best law on the issue of electronic adequacy.

On this issue, I believe that the clear answer is that adoption of UETA would produce substantively less useful and effective rules than exist under current law or under a state enactment of federal standards. Stated simply, in terms of

promoting electronic commerce and protecting consumer interests, the Federal Act is better law.

Rather than examine the entire statutes, I will focus on the major provisions.

A. Basic Rule

The Federal Act provides that electronics cannot be discriminated against solely because they are electronic. UETA does not have the same rule. While the statutory language is identical, UETA only applies if the parties "agree" to conduct a transaction electronically, While the UETA comments suggest a minimalist interpretation of this requirement, the comments are not persuasive about what is an adequate indication of such an agreement and, in any event, they do not have the force of law. Unlike current law, UETA would inject a new standard or precondition for validation of electronics. There is no clear reason why this should be done on an across the board basis.

In fact, UETA does not validate electronics, but rather places many non-waivable limitations on when an agreement to use electronics can be effective in the face of a state law requiring a writing. In the absence of an agreement to use electronics, UETA gives no validation. Even given an agreement to use electronics, UETA limits the effect of that agreement.

This issue favors retaining current law or enacting a state version of the federal rule.

B. Attribution.

UETA deals with when a record or signature is attributed to a party, while the Federal Act does not. However, the UETA rule is simply that attribution must be proven. There is little doubt that this is the same rule as exists today without UETA. There is no benefit in stating the obvious in a statute.

This issue gives no advantage to either alternative.

C. Retainability

Both the Federal Act and UETA deal with whether an electronic record must be retainable. The Federal Act allows, but does not require, a state to reject an electronic record that "is not in a form that is capable of being retained and accurately reproduced *for later reference* by all parties or persons who are entitled to retain the contract or other record."[1] UETA requires

1. Federal Act 101(e) (emphasis added).

that a record be in a form capable of being retained by the *recipient at the time of receipt.*

The UETA rule would invalidate any record that the individual recipient's system cannot retain at the time, either because of technological incompatibility or because the recipient is using a hand held system without a memory or printing capacity. The Federal Act rule provides greater flexibility and requires merely the capability of later access.[2]

In an era of rapidly changing and miniaturizing technology, the greater flexibility of current law in light of the Federal Act is preferable.

D. Inhibiting Retention.

UETA provides that: "An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record."[3] This renders the record inadequate to meet a writing requirement even though the parties agreed to use electronics. What does "inhibit" mean? UETA further states that if "a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient."[4] One could read this as a restatement of the prior rule, but the language is not restricted to cases where law requires a writing and the statutory language might imply a broader scope. Does this language affect the case where underlying law does not require a writing? Does the language apply where the *performance* of a contract involves an electronic record (e.g., a vendor transfers an electronic version of a motion picture which cannot be copied or retained)? The answers should be no.

---

2. The correct interpretation is that the states can require that the record must have been *capable* of being retained and reproduced when the relevant transaction or legal effect occurred. Whether each of the parties *in fact* retained or reproduced it, or even used a device which at that time could do so, is not material. This is supported by comments of a primary sponsor involved in the Federal Act: "With respect to Section 101(e), the actual inability of a party to reproduce a record at a particular point in time does not invoke this subsection. The subsection merely requires that if a statute requires a contract to be in writing, then the contract should be capable of being retained and accurately reproduced for later reference by those entitled to retain it. Thus if a customer enters into an electronic contract which was capable of being retained or reproduced, but the customer chooses to use a device such as a Palm Pilot or cellular phone that does not have a printer or a disk drive allowing the customer to make a copy of the contract at that particular time, this section is not invoked. The record was in a form that was capable of being retained and reproduced by the customer had it chosen to use a device allowing retention and reproduction."

3. UETA § 8(a) (2000 Official Text).

4. *Id*. 8(e).

Current law under the Federal Act does not create these new, indeterminate rules.

On this issue, the clear preference is for current law in light of the Federal Act because it avoids uncertainty an avoids reaching into areas better handled by concepts of good faith, fraud and the like.

Electronic Agents

Both statutes validate the actions of "electronic agents" and use virtually identical language in doing so. This creates or supports no reason to change current law under the Federal Act.

Preservation of other Law

The Federal Act states that it does not alter any other requirement of existing law other than the requirement or a writing or a written signature.[5]

UETA contains no statement like that in the Federal Act, but adopts the concept in a different manner. The UETA Comments describe UETA as purely a *procedural* statute that does not alter substantive law. Thus, substantive policies in other law are preserved.[6] Further, UETA Section 8(b) outlines several rules that in part preserve and in part alter laws and regulations of a type dealing with writings. The attempt to list specifics of other law that are not affected creates a risk of both over- and under-inclusiveness.

The balance between a general statement of preservation of other rules and the approach taken in UETA is not entirely clear, but current law in light of the Federal Act avoids many of the risks taken in the UETA approach.

Consumer Issues

UETA does not have special consumer rules.

The Federal Act (101(c)) deals specifically with the transition from paper to electronics in cases where state law requires disclosure in writing related to the transaction involving consumers. These elaborate rules require informed consent by the consumer and a procedure that ensures that the consumer is in fact able to receive the electronic records it has agreed to receive.

While the procedures are somewhat cumbersome, from a consumer protection standpoint, current law under the Federal act is clearly a preferable, firm step to protect against unwarranted claims of assent to using electronic disclosures.

5. Federal Act 101(b).
6. UETA § 3(d).

This factor weighs in favor of the current law under the Federal Act.

Mistakes

UETA contains a non-waivable rule that allows an individual to rescind and avoid the effect of an agreement entered into by mistake in a transaction with an automated system. The rule applies to consumer and to business-to-business transactions.

The Federal Act has no similar provision, leaving the issue to state law of mistake and the like.

The UETA rule may be appropriate for consumer transactions, but is an entirely inappropriate rule in the realm of commercial transactions between businesses, where just-in-time inventory and similar systems can create significant reliance costs that are not factored into the UETA rule.

This factor favors retaining current law in light of the Federal Act.

Deemed Sent and Received

UETA contains various rules about where, from, and when an electronic message is deemed to have been sent or received. The effect of these rules is to create presumptions about the location of sending and receipt that may or may not reflect ordinary expectations. The effect of these provisions is not clear, but likely affects tax, jurisdiction and other issues.

The Federal Act contains no presumptions about from where a message is deemed sent or received.

The Federal Act rule is preferable.

Summary

The substantive rules of the two statutes clearly favor retention of current law under the Federal Act. Moving to a pure version of UETA would have many detrimental effects on electronic commerce in Texas with no clear, off-setting benefits.

APPENDIX 2

SUBSECTION (C) OF E-SIGN

(c) Consumer Disclosures.

(1) CONSENT TO ELECTRONIC RECORDS.—Notwithstanding subsection (a), if a statute, regulation, or other rule of law **requires** that **information** relating to a transaction or transactions in or affecting interstate or foreign commerce **be provided or made available** to a **consumer** in **writing**, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing **if**—

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement—

(i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal;

(ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties' relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an

electronic record, and (II) whether any fee will be charged for such copy;

(C) **the consumer**—

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) **consents electronically, or confirms** his or her consent **electronically**, in a **manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information** that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record—

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).

(2) Other Rights.—

(A) PRESERVATION OF CONSUMER PROTECTIONS.—Nothing in this title affects the content or timing of any disclosure or other record required to be provided or made available to any consumer under any statute, regulation, or other rule of law.

(B) VERIFICATION OR ACKNOWLEDGMENT.—If a law that was enacted prior to this Act expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt (whichever is required).

(3) EFFECT OF FAILURE TO OBTAIN ELECTRONIC CONSENT OR CONFIRMATION OF CONSENT.—The legal

effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).

(4) PROSPECTIVE EFFECT.—Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer in accordance with paragraph (1) prior to implementation of the consumer's withdrawal of consent. A consumer's withdrawal of consent shall be effective within a reasonable period of time after receipt of the withdrawal by the provider of the record. Failure to comply with paragraph (1)(D) may, at the election of the consumer, be treated as a withdrawal of consent for purposes of this paragraph.

(5) PRIOR CONSENT.—This subsection does not apply to any records that are provided or made available to a consumer who has consented prior to the effective date of this title to receive such records in electronic form as permitted by any statute, regulation, or other rule of law.

(6) ORAL COMMUNICATIONS.—An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law.