CLEAR SIGNATURES, OBSCURE SIGNS*

ADAM WHITE SCOVILLE**

CONTENTS

* This Article is published simultaneously by the *Cardozo Arts & Entertainment Law Journal* and the *Intellectual Property and Technology Forum at Boston College Law School.* Any updates and addenda subsequent to publication will be posted with the article on the *Forum*, at <http://www.bc.edu/iptf/articles>.

** B.A., 1994, Yale University; J.D., 1999, Boston College Law School; Director (1997-99), *Intellectual Property and Technology Forum at Boston College Law School.* Questions or comments on this work or its underlying subject matter are welcome. E-mail the author at <adville@aya.yale.edu>. Thanks to Alfred Yen, Boston College Law School, Alan Davidson, the Center for Democracy and Technology, and Anthony Ellsworth Scoville for their insightful suggestions and comments, and to Shabbir Safdar of mindshare Internet Campaigns, L.L.C, for assistance with the cryptography demonstration exhibits. As always, for their support and inspiration, I am indebted to my family and friends, particularly Susan Cooke Kittredge, Ann Curtiss Scoville, Jane White Cooke, and Alistair Cooke.

I. Introduction

There are two kinds of digital signatures: signatures good enough for a six dollar trade among friends, and signatures good

enough for a six figure trade between strangers.[1] This Article considers both, from the digital equivalent of an initialed placemat to secure verification techniques more like notarizations. Nationally and internationally, diverse groups and bodies have been propelling the development of digital signature and certificate authority regulation and legislation. This Article examines the need for such legislation, questioning the assumption that current law presents, at best, uncertainties or, at worst, outright barriers to the use of electronic records and signatures. This analysis attempts to determine the extent of such uncertainty or conflict, by examining case law, as well as the most crucial technological and policy issues that face the drafters of digital signature legislation. Finally, the major statutes, drafts, and model laws are evaluated with regard to their efficacy in addressing the concerns so identified.[2]

The fundamental question legislation drafters face is the same question courts face: under what circumstances are electronic records and signatures as trustworthy as traditional writings and signatures? Beyond this question, however, many groups have also considered whether there is a need to legislate proactively in order to encourage the use of the more secure varieties of electronic signatures and to stimulate electronic commerce. To analyze fully the existing common-law environment for the treatment of digital records and signatures, one would ideally examine cases involving both low security records (e.g., a faxed signature, a name in text at the end of an e-mail) and records protected by elaborate security measures (particularly those that have been cryptographically signed). Unfortunately, while the law has long dealt with the application of new technologies by which non pen-and-ink signatures are used, as of yet there are no cases ruling on the per se validity of writings or signatures where a message was cryptographically signed.[3]

Thirteen states have digital signature statutes that apply generally to public and private settings; at least six have already passed "comprehensive" legislation also including the regulation of certificate authorities.[4] Pioneered by the Utah Digital Signature Act,[5]

---

[1] Adapted from BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C at xix (2d ed. 1996) ("There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.").

[2] No attempt is made at presenting a comprehensive survey of all relevant proposals and statutes in existence. Rather, the goal is an analytical comparison of the major paradigms that have been proposed.

[3] *See infra* text accompanying notes 85-86.

[4] *See* McBride Baker & Coles, *Scope of Authorization to Use of Electronic Signatures in Enacted Legislation* (last modified Apr. 5, 1999) <http://www.mbc.com/legis/table01.html>.

the "comprehensive" laws set precise rules governing the validity of signatures, the issuance and revocation of certificates, and the regulation of certificate authorities. In addition, a growing number of states have enacted limited statutes specifying only a vague outline for digital signature validity and delegating broad rulemaking authority to executive agencies.[6] Various guidelines and model laws have also contributed greatly to the evolution of state laws in this area, including efforts by the American Bar Association, the National Conference of Commissioners on Uniform State Laws ("NCCUSL"), which is preparing a Uniform Electronic Transactions Act, and the United Nations Commission on International Trade Law ("UNCITRAL").

Several subordinate concerns must also be considered in the preparation of digital signature laws and drafts. As should be evident from the discussion herein, different types of electronic "signing" yield different levels of reliability. Drafters must acknowledge that it may be necessary to abandon bright line, "yes or no" rules in order to treat different kinds of signatures appropriately in all cases. This may mean leaving digital signatures equivalent to normal, signed documents in some cases and attaching evidentiary

---

The states with "comprehensive" certificate authority legislation are Minnesota, Mississippi, Oregon, Utah, Washington, and West Virginia. *See id.* The states with other, generally applicable digital signature legislation are Alaska, Florida, Georgia, Illinois, Kansas, Kentucky, New Hampshire, Missouri, Nebraska, Oklahoma, South Carolina, Tennessee, and Virginia. *See id.* In addition to these statutes of general applicability, nine states (Arizona, California, Idaho, Indiana, New Mexico, North Carolina, North Dakota, and Texas) have laws validating electronic signatures in communications with state government, and another fourteen (Alabama, Colorado, Connecticut, Delaware, Iowa, Louisiana, Maine, Maryland, Montana, Nevada, Ohio, Rhode Island, and Wyoming) provide for the use of electronic signatures for specific applications (for example, U.C.C. filings). *See id.* Vermont and Hawaii only have laws studying the issue, and only six states (Massachusetts, Michigan, New Jersey, New York, Pennsylvania, and South Dakota) have no enacted law addressing digital signatures in any context. *See id.* For a frequently updated catalog of enacted and pending digital signature legislation nationwide, see McBride Baker & Coles, *Summary of Legislation Relating to Digital Signatures, Electronic Signatures, and Cryptography* (last modified Apr. 12, 1999) <http://www.mbc.com/ds_sum.html>.

5 UTAH CODE ANN. § 46-3 (1998).

6 As mentioned below, when discussing different signing techniques, some commentators refer to cryptographic signatures as "digital signatures" and use "electronic signatures" for other types, or as a generic term to avoid confusion. As an unrelated shorthand, I will use the term "digital signature legislation" to refer generically to statutes that address the legal validity of digital or electronic signatures, and "certificate authority legislation" in reference to statutes that also set out a regulatory infrastructure for certificate authorities and a public key infrastructure involving trusted third parties. Certificate authority legislation generally but not always, *see infra* Part VI.C.1 (discussing the Secure Public Networks Act), also addresses the legal validity of signatures. A third type of statute, which might be dubbed "government use" statutes, deals with government use and acceptance of electronic signatures in inter-agency communications and selected citizen and business filings. As these statutes are of very narrow scope, they are generally ignored, with the exception of the California statute (which has been a model for many broader statutes), and Federal government use statutes, where unusual concerns apply. *See infra* Parts VI.A.2 & VI.C.

presumptions to others, even within the same statutory scheme. Some of these protections may be appropriate for generically defined signatures, and other measures may be appropriate only when specific, proven technologies, such as public key encryption, are used. In addition, digital signature laws must avoid interfering with the validity of electronic authentication procedures agreed to by contract, and with the validity of already-valid traditional signatures.

Drafters concerned solely with removing impediments in preexisting laws may view the question of enhanced protection for secure signatures very differently from those who think the legal environment should proactively encourage the use of secure authentication methods. Either viewpoint may be appropriate, but drafters must be aware of their objectives. Moreover, digital signature statutes would be most effective if they were uniform and compatible with the laws of other states and nations. Yet, this goal must be balanced against preserving decentralization of regulation in order to allow experimentation and evolution in this nascent industry, and to avoid the negative privacy implications of an overly centralized infrastructure.

In short, the legal landscape is treacherous. It is therefore critical that any legislation be made with deliberate caution, adherent to two basic, guiding principles. First, given the uncertain environment, legislation must be narrowly tailored to address specific legal needs and obstacles. Second, the level of legal protection and recognition granted signatures must be no greater than is commensurate with the security and reliability provided by the weakest form of signature to qualify for such protection.

II. Background: Technical Foundations of Digital Authentication

On one extreme, ad hoc methods of electronic authentication that are expedient, but not secure, are being used with increasing frequency. On the other extreme, however, secure methods of electronic signing based on public key cryptography are emerging. It is helpful, therefore, to examine the technology behind cryptographic authentication and the basis for claims regarding its reliability.

Cryptography is a process by which data (which could be anything from a text e-mail message, to a digital picture, to a binary software program, to streaming data of a real-time digital phone conversation) is kept secret by scrambling it so as to render it

unintelligible gibberish to eavesdroppers.[7] *Encryption*, specifically, is the process whereby an *algorithm* (a series of mathematical processes) is applied to this data, or *plaintext*, producing the scrambled *ciphertext*.[8] Through an inverse mathematical process, namely *decryption*, the ciphertext may be retransformed into the original plaintext.[9]

Imagine that Alice and Bob wish to communicate by encrypted messages.[10] In order to keep an eavesdropper, Eve, from performing the decryption process herself, either the algorithm itself must be kept secret (which is almost never done today because the algorithm's use would be limited to one group of communicants), or the algorithm's results must depend on the insertion of another string of data, namely the *key*, which is kept secret.[11]

There are two kinds of encryption: *symmetric* (also known as *single key*) encryption and *public key* (or *asymmetric*) encryption.[12] Symmetric cryptography is what most readers will think of as classic, simple encoding; the same key is used to encrypt the plaintext as to decrypt the ciphertext.[13] A protocol for using symmetric cryptography would be that: (1) Alice and Bob agree on an algorithm; (2) they then agree on a key (or one of them dictates both); (3)

---

7 *See* SCHNEIER, *supra* note 1, at 1. This Article does not attempt to explain general cryptographic principles or the primary cryptographic function of keeping messages secure from unauthorized access. Rather the focus is on such technical details as are necessary to explain (in as much brevity as is possible) the cryptographic signing of data for purposes of authentication, integrity verification, and non-repudiation. For an encyclopedic and commendably comprehensible explanation of cryptographic principles and application, Bruce Schneier's *Applied Cryptography* is deservedly the standard authority. *See id.* This Article, likewise, seeks to steer clear of the main "encryption debate" over the balance between law enforcement access to encrypted data and civil liberties concerns, even though at times digital signature law has inappropriately been used as a leverage point in that battle. *See infra* Part VI.C.1 (discussing Senate Bill 909, the McCain/Kerrey Secure Public Networks Act). For a detailed and admirably detached background discussion of the policy framework in which encryption resides, including discussion of export regulations, electronic surveillance statutes, and key escrow encryption, see COMMITTEE TO STUDY NATIONAL CRYPTOGRAPHY POLICY, NATIONAL RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY (Kenneth W. Dam & Herbert S. Lin eds., 1996) [hereinafter NRC CRISIS REPORT].

8 *See* SCHNEIER, *supra* note 1. Schneier notes that, according to the relevant International Standards Organization standard, *encipher* and *decipher* are technically preferable terms, as "encryption" and "decryption" refer in certain cultures to corpses. As this Article is intended for an American legal audience by virtue of its discussion of domestic law, the far more common encrypt/decrypt will be used, with no disrespect intended.

9 *See id.*

10 This Article will follow the convention in cryptographic literature of referring to communicants as Alice and Bob (and where more parties are necessary, Carol and Dave). In addition, where appropriate, Eve is a relatively passive eavesdropper, while Mallory (sometimes known as Mallet) is a cracker with more malicious intent, and Trent is a trusted third party arbitrator (such as a certificate authority). *See id.* at 23.

11 *See id.* at 3.

12 *See id.* at 5.

13 *See id.* at 29.

Alice encrypts the message using the agreed upon key; (4) Alice then sends the ciphertext to Bob; (5) Bob then decrypts it with the key.[14] The message is secure if step four only (or perhaps steps one and four) is done in public, where Eve can listen. However, if step two, the selection of the key, is also done in public and not by a secure channel, then Eve overhears which key is being used and can decrypt the ciphertext just as well as Bob can.[15] Symmetric key cryptography is analogous to a combination safe, where both the person putting items into the safe and the person taking them out of the safe must be able to open the combination lock.[16]

In a public key system, however, Bob generates two different but corresponding keys.[17] One key can encrypt (the *public key*) and one (the *private key*) can decrypt the first key's resulting ciphertext.[18] Bob can now publish the public key for Alice's use in encrypting her message to him, secure in the knowledge that Eve (who lacks the *private* key) cannot decrypt the message.[19] Public key encryption is analogous to a post office box, where anyone can deposit mail once the recipient's specific box number (the public key) is known, although only the box holder with the (private) key can open the box.[20] However, there are two disadvantages to public key cryptography. First, messages must be encrypted for specific recipients' private keys, complicating procedures in the case of communication among groups.[21] Again, to analogize, where one message could be put in a safe for everyone with the combination to read, Alice must put separate copies of the message in Bob's,

---

14 *See id.* at 28.

15 *See id.* at 28-29. This implies a paradox like that of the old lady who challenged a scientist, who had lectured on the structure of the solar system, by insisting that the world is a flat plate on the back of a tortoise. The scientist of course rebutted, asking what then was the tortoise standing on. The lady replied, "You're very clever . . . but it's turtles all the way down!" *See* STEPHEN W. HAWKING, A BRIEF HISTORY OF TIME 1 (1988). If the need for a secure protocol to exchange the key (in order to make a secure connection) really is "turtles all the way down," then symmetric systems are only useful when the parties have met in person to do so.

16 *See* SCHNEIER, *supra* note 1, at 31.

17 *See id.* at 31-32.

18 *See id.* Public key cryptography rests on the fact that multiplication is a one-way function; it is very easy to multiply two prime numbers together but, so far as we know, very difficult to determine the prime factors from the result without trying out all the primes. The private key is the two prime factors and the public key is the product. Given a public key of 35, the private key would be analogous to the combination of 7 and 5, although we would have had to try 2 and 3 first, which is why very large prime numbers are used. Just as we can deduce 7 and 5 from nothing but the public key 35, so can any such private key be deduced; the problem is that, with sufficiently large numbers, it takes so long to try the factors that to do so is computationally infeasible with current or projected computer power. *See* NRC CRISIS REPORT, supra note 7, at 376.

19 *See* SCHNEIER *supra* note 1, at 32.

20 *See id.* at 31.

21 *See id.* at 33.

Carol's, and Dave's post office boxes (i.e., encrypt the message separately with each of their public keys), so that they all can read it. Second, processing encryption or decryption with a public key algorithm is roughly a thousand times as slow as with a symmetric algorithm.[22]

Therefore, in practice, programs that claim to use public key encryption are really hybrid systems.[23] In these systems, Alice and Bob have their respective public keys, but they are used only to encrypt and transmit securely a *symmetric* encryption key called, in this context, a *session key*. A session key will be used to encrypt and decrypt the content of the communication, but will not be reused after the specific communication is completed.[24] This system avoids the paradox of symmetric systems needing a secure channel to communicate keys, and avoids the slowness of using public key cryptography alone.[25]

A. *The Use of Encryption for Authentication*

When public key cryptography is used in reverse, with the *decryption* key now made public and the *encryption* key held secret, the result is a message that anyone can verify only to have come from, or been *signed* by, its bona fide sender.[26] The message is linked to whomever holds the private key corresponding to the public key that the recipient has obtained.[27] Therefore, if the recipient personally knows that the sender is associated with the private key, this is enough to link the sender with the message.[28] Where Alice and Bob do not know each other, they call beforehand on Trent, whom everyone trusts implicitly. Trent signs each of their public keys, certifying that he knows that the real Alice controls the private key labeled "Alice's Key," the real Bob controls "Bob's Key," and so on.[29] In large scale networks of encrypted communications, "Trent" is a *certificate authority* ("CA"), a private or governmental entity that has itself verified Alice's identity.[30] A

---

22 *See id.* Public key encryption is also somewhat more vulnerable to attack in certain specialized cases.

23 *See id.* at 32-33.

24 *See id.*

25 *See id.*

26 *See id.* at 37. In some algorithms, such as RSA (named after its three inventors: Ron Rivest, Adi Shamir, and Leonard Adleman), either the public key or private key is capable of encrypting a message. In other systems, most notably PGP ("Pretty Good Privacy"), two algorithms are actually used, one for encrypting messages, and one for signing. The user has a pair of keys, one for each algorithm.

27 *See id.* at 33.

28 *See id.*

29 *See id.* at 37.

30 This would be done by verifying, for example, the link between the key and Alice's e-

widespread system of certificate authorities and the procedures for verifying a certification is known as a *public key infrastructure* ("PKI") or *key management infrastructure* ("KMI").[31]

Once again, the slowness of public key cryptography makes it impractical to perform this process on large amounts of data. In practice, the sender actually signs only a mathematical output of the message, called a *hash*, which is dependent on the content of the message.[32] A hash function produces a finite result from an input plaintext of any size, but that output will change if the message is changed, even slightly.[33] One example of a rudimentary (and insecure) hash function would be to add up the ASCII values (in a standard ASCII text file, each letter, number, or symbol is represented by a number between 0 and 128) of the message text, and then keep only the last three digits (a number from 000-999) as the hash value. Only one in a thousand messages would share the same hash value, so one has some basic assurance that the message received is exactly the same as the one sent.[34] Of course, cryptographic hash functions are much more complex and secure.[35] A side advantage of signing a hash value as opposed to the

---

mail by sending the signed key to Alice's stated e-mail address, or by requiring Alice to bring her key to the local office in person and show proof of whatever is being certified, be it her identity, her age or her creditworthiness. *See id.* at 185-87.

[31] *See id.* In the absence of an established PKI, the widely used program PGP relies on a somewhat more ad hoc method known as the *web of trust*. Alice solicits as many acquaintances as possible to sign her public key, hoping that eventually, by a kind of "six degrees of separation" logic, any stranger with whom she communicates will know and trust someone (who trusts someone) who has signed her key. *See* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 56 n.26 (1996). While this may be adequate for identification purposes, it is obviously deficient when one wants to know not only that Bob is not Mallet under an alias, but that Bob will be good for the bill for the $1200 in satin undergarments he just ordered from the Victoria's Secret web store. Froomkin's article makes an excellent preliminary examination of the mechanics of certificate authorities and their legal environment under common law theories of tort and contract prior to the widespread proliferation of digital signature legislation.

[32] *See* SCHNEIER, *supra* note 1, at 38-39.

[33] *See id.* at 30.

[34] *See id.* at 30-31, 38-39. My example of a simple checksum is poor in that it is feasible to alter a given message and then make further reciprocal alterations to correct any change in the checksum. Cryptographic hash algorithms are one-way functions. This means that, while there are still many messages sharing any given hash value, it is computationally infeasible to find them. For all practical purposes, the value is unique and, therefore, the message must not have been altered.

[35] *See id.* Digital signatures usually also include a time stamp as a unique identifier. Without such an identifier, as Schneier points out, *see id.* at 38, if Alice gives Mallory a digital check, Mallory could deposit the check on Tuesday, and then deposit it (technically, a copy, but as with all digital copies, indistinguishable from the original) again, perhaps in another account, later on. With the time stamp identifier, the second bank would look up the identifier in a digital check clearinghouse, see that the check has already been cashed, and refuse payment. *See id.* at 38, 40. Time stamps could also be used to keep Alice from unjustly refusing payment by saying that her private key had been compromised, and that someone else must have signed the check.

entire message is that, unless the sender separately chooses to encrypt the message, the actual text of the message still appears as plain, unaltered text.

B. *Examples of Encryption and Cryptographic Digital Signing*

Exhibit One is an example of a cryptographic public key generated using Pretty Good Privacy.[36] Exhibit Two looks like a normal e-mail message except that a hash value has been produced and encrypted in order for the sender to sign the message digitally; a small tag indicates the beginning boundary of the data to which the hash was applied. In receiving this message, I used the sender's public key (quite similar in its gibberish appearance to my own) and was greeted with an alert signal saying that the signature had been successfully verified, and listing the time of the signing. In Exhibit Three, the same message from Exhibit Two was sent again, except that not only was it signed using the sender's private key, but the result (including the signature) was encrypted using my public key as found in Exhibit One.[37] The message in Exhibit Four is identical to the message sent in Exhibit Two (and Exhibit Three) except for one character; the price of the software license is $4500, not $14,500. Note that in the signature, twenty-six of the first thirty-two characters are the same as in the signature in Exhibit Two, but after that, none of the data is the same. If I were to try to act more like Mallory than like Bob, and had received Exhibit Two but altered it and claimed to owe $10,000 less than in actual fact, my fraud would easily be discovered when the signature is found not to match what was expected in Exhibit Four.

C. *Other Technologies for Creating Secure Signatures*

Some have argued that other technologies might be able to create digital signatures of approximately equal security to cryptographic signatures, although none of these techniques has received

---

[36] Note that public keys under some protocols are much shorter than this one (belonging to the author) because PGP 5.0 and higher uses separate algorithms for encryption and for signing, so that the key contains not one, but a pair of public keys. In addition, PGP's public keys store information about every time the key was signed by a third party (several times in this case) in order to facilitate web of trust verification. In a public key infrastructure, the key would contain the signature of the allegorical Trent as the certification authority, as well as what information was used to verify my identity in the certification procedure. It would possibly also include a recommended limit as to how big a transaction should be entered in reliance on the certificate, given the level of verification that went into the certificate's issuance.

[37] If the message in Exhibit Two had been signed in its entirety, as opposed to merely the hash value being signed, Exhibit Two would have looked like a sibling of Exhibit Three, rather than a mostly recognizable message.

the degree of theoretical scrutiny that cryptography has received. One state has gone so far as to declare that "Signature Dynamics" is an acceptable technology for digital signing.[38] Signature dynamics systems make a digital record of a manual signing (including not just the shape, but the speed from stroke to stroke, pressure, angle of pen, and other identifying characteristics of the way a person signs his or her name) which can be transmitted to authenticate a digital document.[39] In addition, other forms of biometric authentication may be incorporated into digital authentication protocols. For example, a biometric fingerprint or eye scan authentication system might be used in a hybrid system instead of a passphrase to protect the private key in a cryptographic system.[40] Many of these methods have different levels of reliability and utility for digital authentication.[41] Likewise, companies involved in biometric identification admit that while units are sophisticated in detecting fraudulent identifiers, such as recordings of voices or copies of fingerprints, they are vulnerable to the tapping of the output data of the biometric reader as it is transmitted for verification.[42] As such, these other methods serve more appropriately as a warning that states should anticipate the development of other secure technologies, than as an indication that such other technologies are ready for prime time at present.

III. Clarifying Obscurity in Law - Policy Objectives Examined in Light of Current Legal Conditions

A. *Literal Constructions and Legitimate Concerns in "Writing" and "Signature" Requirements*

The validity of electronic signatures comes into question because state and federal law are littered with provisions that are contingent on the presence of a document in writing, or the

38 *See* California Digital Signature Regulations, Cal. Code Regs., tit. II, §§ 22000-22005 (1997), *available at* <http://www.ss.ca.gov/digsig/regulations.htm>.

39 *See id.*

40 During the spring of 1998, for example, a bank in Swindon, England, opened ATMs that scan the pattern of account-holders' irises in lieu of requiring personal identification numbers. *See* Kristi Essick, *Iris ID squares off against fingerprint and handprints,* Info World Electric, (June 29, 1998) <http://www.idg.net/idg_frames/english/content.cgi?vc=docid_9-64667.html>.

41 Signature dynamics, for example, can not be performed in real time, and verification requires comparison of the signature dynamic data with data taken from a verified exemplar by a handwriting analyst.

42 *See* Paul Collier, Director of Operations, Identicator Technologies, Inc., Remarks at the Public Forum on Certificate Authorities and Digital Signatures: Enhancing Global Electronic Commerce Conference (July 24, 1997). This is particularly worrying because, while a bank can easily issue a customer a new PIN if hers is compromised, it is, to say the least, more complicated to issue her a new iris, voice pattern, or fingerprint.

endorsement of a writing with a signature.[43] A writing requirement has traditionally sought to insure that the terms of a document can be fixed, and any ambiguities limited to the meaning of the text, rather than to parties' contradictory assertions about what the operative text is.[44] Traditionally, signature requirements have sought, on the other hand, to demonstrate the signer's intent to commit himself to the specific text. With the advent of the first photocopy machine, and then of electronic document storage and transmission, legal documents are made in media where it is possible to make alterations or forgeries that are facially irrefutable. Thus, the enforcement of writing requirements and the enforcement of signature requirements have become intertwined. Likewise, the policy concerns behind them have merged. In addition, statutes increasingly state signing and writing requirements as a single unit, or make them dependent on one another.[45] In other words, the question is seldom whether a given document exists tangibly, or whether a specific text (or other content) can be pointed to (as is the issue with oral statements); that concern is satisfied regardless of whether the document is on paper, or is a fax, an e-mail, or a videotape. Rather, the question raised by the writing requirement is whether the given document is actually *the real* doc-

---

[43] Such requirements are so numerous, perhaps in the tens of thousands, that a practical concern in setting the scope of digital signature laws is a huge "search and replace burden," which would be required if the law applied to all signatures, in order comprehensively to update codified statutes. *See* Memorandum from Ben Beard, Reporter to Electronic Transactions Act Drafting Committee and Observers, at 3 (Aug. 15, 1997), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/ect997.htm> [hereinafter UETA Aug. 1997 Draft Reporter's Memorandum]; INFORMATION TECHNOLOGY DIVISION, COMMONWEALTH OF MASSACHUSETTS, SIGNATURE REQUIREMENTS OR REFERENCES IN THE MASSACHUSETTS GENERAL LAWS, available at <http://www.state.ma.us/itd/legal/toc.html> (listing index of hundreds of signature requirements in Massachusetts law alone).

[44] Under the *Restatement (Second) of Contracts*, a writing is acceptable if it:

> (a) reasonably identifies the subject matter of the contract
>
> (b) is sufficient to indicate that a contract . . . has been made . . . and
>
> (c) states with reasonable certainty the essential terms of the unperformed promises in the contract.

RESTATEMENT (SECOND) OF CONTRACTS § 131 (1978). The Comment to § 131 also states that "[t]he primary purpose of the Statute is evidentiary, to require reliable evidence of the existence and terms of the contract . . . ." *Id.* cmt. c.

[45] *See, e.g.,* U.C.C. § 1-206(1) (1995) (stating that the sale of personal property over $5000 requires "some writing which . . . is signed by the party against whom enforcement is sought . . . ."); *id.* § 2-201 (1995) (stating that a contract for sale of goods over $500 requires "some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought . . . ."). In addition, the U.C.C. manifestation of assent clause (which is analogous to a signature or attestation requirement) is linked to the reasonableness of the medium on which the assent is made: "an offer to make a contract shall be construed as inviting acceptance in any manner and by any medium reasonable in the circumstances." U.C.C. § 2-206 (1995). Presumably, if the U.C.C. Statute of Frauds applied (as in § 2-201 or § 1-206(1)), a signed writing would be required to make the medium of acceptance "reasonable."

ument, the *document of significance*.[46] After all, the significance of one document over another is that it has been sanctioned by a particular person, usually by signing it. Likewise, the general trend in common law and statutes is to recognize that a signature may be, for example, "any symbol executed or adopted by a party with present intention to authenticate a writing."[47] Therefore, the challenge to the signature is relative to the accompanying writing and whether that text is the one the signer intended to authenticate.

Under all of these concerns, a manual (ink) signature on paper is ideal, because of the difficulty either in mechanically reproducing the signature without the reproduction being obvious, or in changing the pre-printed text on the same physical piece of paper. Nonetheless, it is often commercially reasonable to rely on other media where one lacks either the paper (e.g., e-mail, or digitized signature for a UPS package) or the manual signature (e.g., fax or rubber-stamped signatures). Writing and signature requirements have, therefore, commonly been used for attacking an electronic (or electronically transmitted) record where the attack would not easily fall under hearsay or the best evidence rule,[48] and where authentication requirements, for example those in rules 901 to 903 of the *Federal Rules of Evidence*, provide too low a threshold to address these concerns.[49] In short, signature and writing requirements exist to acknowledge: (1) that some records are unreliable because they are easy to forge; (2) that other threshold tests have been eviscerated; and (3) that the opponent is unlikely to be able to offer a smoking gun to prove forgery.[50]

---

46 With this talk about the "real document" it may appear that objections either under the hearsay exclusion or the "best evidence" (more accurately the original document) rule are implicated. This is misleading. Hearsay would not apply because the proponent is not claiming that the document in question is a trustworthy "copy," but that it is the original. As to the best evidence rule, the document would likewise be acceptable for the same reason: either no "original" manual signature exists (as in telex or e-mail) or it is in the possession of the opponent (as in a fax). For a more thorough discussion of the application of hearsay and the best evidence rule to electronic documents, see BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE: EDI, E-MAIL, AND INTERNET: TECHNOLOGY, PROOF, AND LIABILITY chs. 9 (hearsay) & 10 (best evidence rule) (2nd ed. Release 2, Nov. 1996).

47 U.C.C. § 1-201(39) (1995). *See also* Ames v. Schurmeire, 9 Minn. 221 (1864) (stating that the "written signature" requirement is satisfied by a manual signature, or a "proper mark," if the signer cannot write).

48 *See* WRIGHT, *supra* note 46.

49 *See id.* Statutory requirements of an "original" do present an obstacle, and several digital signature laws do address the question of when a retained computer record is legally an "original." However, such requirements are much rarer and raise the same general issues as writing and signature requirements and will not need to be addressed in detail here.

50 *See* RESTATEMENT (SECOND) OF CONTRACTS § 131 cmt. c (1978) (stating that the Statute of Frauds signature requirements seek "to prevent enforcement through fraud or perjury of contracts never in fact made. The contents of the writing must be such as to make successful fraud unlikely . . . ."). At best, the opponent will have his differing copy of the

Challenges to documents or records, made under legal writing or signature requirements, can be divided into two types. The first type of challenge occurs when the litigant does not contest that the specific document or record is authentic, or that she intended to bind herself in signing it. Rather, she challenges the writing or signature simply on the basis that the statute explicitly prohibits such documents from being enforced (and perhaps that she relied on this unenforceability). This is a purely formalistic argument, because invalidation of the document would exceed the underlying purpose of the statute, which exists because (1) some manifestation of the actor's intent is necessary to bind her to the specific terms of the writing, and (2) a signed writing is a good indication of such intent. In this type of case, that intent is not contested, so there is no need for strict enforcement of the writing or signature requirement.[51] This type of challenge seems more prevalent in appellate case law (leading some to the conclusion that the Statute of Frauds is somewhat of a hollow shell).[52] However, it is not the type of challenge with which we are primarily concerned.

The second type of challenge asserted regarding writing and signature requirements goes more to the purpose of the requirements themselves. These challenges involve cases where the purported "signer" of the document protests that, *despite the document's presence*, the document is not a concrete manifestation of the terms of the agreement.[53] The document allegedly does not represent the agreement because either the content or the signature is easy to forge (and was forged), or because the marks claimed to constitute a signature are bona fide, but do not sufficiently demonstrate the signer's intent to be bound. This is really a *substantive* attack under the statute, which functions like a presumption of the document's *invalidity*. This presumption relieves the purported signer of the burden of affirmatively proving the forgery once the concreteness of the writing or the intent to be bound have been sufficiently placed at issue.[54]

---

document, and the court would have no means to tell which is the forgery. At worst, the opponent will have only his word that the document he signed was substantively different from that offered.

[51] While the requirement could also serve as a punitive way of encouraging the use of signed, written instruments, this policy seems to have been adequately served in the cases discussed *infra* Parts IV.B-C., by construing the signature requirement as an obstacle to the admission *only once the signer's intent has been placed in issue.*

[52] *See infra* note 84.

[53] *See* RESTATEMENT (SECOND) OF CONTRACTS § 131(c) (1978).

[54] In essence, the Statute of Frauds functions first as a presumption (through the modern, low threshold requirements) that the document is valid. This presumption operates until the opponent of the document, the purported signer, meets some burden of produc-

B. *Treatment of Informal "Signings": The Digital Placemat*

Electronically signed documents are usually either much less reliable than written signatures in the security they offer against forgery, or much more reliable, but rarely in between. An electronic signature could be a certified cryptographic signature of the kind detailed in the first section, but it could also be the signer's name in ASCII at the end of an e-mail, or the scanned image of a signer's signature found in a fax or a graphics file.[55] When one signs a check at a grocery store, the store has certain indications of the signature's validity or enforceability. The pre-printed check may at least indicate that the signer has a bank account, and indicates how to contact the bank to verify this fact. The pre-printed check may also give an address, useful for tracking down the signer. In addition, the cashier can demand photo identification which would itself: (1) confirm the name and address information; (2) provide visual verification that the signer at the counter is the person named on the checks; and (3) provide a signature exemplar for informal signature comparison.[56] None of these verification methods necessarily exist with the informal electronic signatures mentioned above.[57] Yet in the paper world, fortunes have been validly signed away on the back of airport diner placemats (particularly where the signer admits the signing, as where a third party is the one challenging the transfer, or the

---

tion as to the lack of the document's concreteness or the signer's intent. This may be a low burden if it is met simply by the opponent testifying that he did not intend to be bound. Once this burden has been met, a reverse presumption of the document's invalidity is raised.

The current draft of proposed revisions to U.C.C. Article 2 reflects this structure. Proposed language in the U.C.C. Article 2 Statute of Frauds states:

> A contract for the price of $5,000 or more is not enforceable . . . *against a person that denies facts from which an agreement can be found*, unless there is a record authenticated by the party against which enforcement is sought which is sufficient to indicate that a contract has been made.

U.C.C. § 2-201 (Draft Revision, Feb. 1999) (emphasis added).

55 As a term of art, cryptographic signatures are sometimes known as "*digital* signatures" and less secure ones are known by contrast as "*electronic* signatures," a distinction which will generally be followed, if not slavishly so.

56 The security in the check rests in the ability for on-the-spot verification, not in the increasingly remote possibility that the signature on the check will be verified against the signature on file at the bank. To put in perspective concerns about the security of digital authentication techniques in comparison to the fundamentally insecure methods used in paper world banking, see Ronald J. Mann, *Searching For Negotiability In Payment And Credit Systems,* 44 UCLA L. REV. 951 (1997).

57 An e-mail may provide only information to indicate a "virtual" address which might, with some effort, be traced to an individual, and a fax must, under the Junk Fax Law, provide a station identification (*sometimes* the sender's name) and fax number of the sender. *See* Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (1998) ("Junk Fax Law"). Neither of these pieces of information is instantly useful to the recipient.

signer challenges the instrument on other grounds).[58] Where time is of the essence, parties sign documents and fax them back (sometimes, but not always, promising to send an original by mail); both the signer and the recipient consider themselves bound when the fax is transmitted, not when the hard copy is received by mail.

The question of the signer's intent to be bound, which is critical with ad hoc, informal documents, is whether the purported signer "actually did put his name there." This is not always an easy determination to make. For instance, Exhibit Five is a letter signed by "William J. Clinton" that, among other things, memorializes an employment contract for more than a year in length. In all facial respects it satisfies writing and signature requirements in the Statute of Frauds; it clearly is a writing, and William J. Clinton could not deny that this is his signature, for it is. If Mr. Clinton admitted to the writing, as in an action by Alice claiming the job should have been hers, the party challenging the document would lose in short order. A digital signature law clarifying that "a record may not be denied legal effect, validity, or enforceability solely because it is in the form of an electronic record" and that "a signature may not be denied legal effect, validity, or enforceability solely because it is in the form of an electronic signature"[59] only reiterates the result we would have courts reach, by reasoning that the record is valid where the party intended to be bound under existing law.

By this point, however, we are beginning to suspect this Mallory character, and we would be "shocked, *shocked* to learn"[60] that Mallory fabricated the document from one of thousands of the President's signatures found at the end of Executive Orders and available in impeccably reproducible form through the Government Printing Office's web site.[61] If Mr. Clinton were to challenge the document as a fabrication under writing or signature requirements, the right result should likewise be reached under existing law: either it fails to satisfy the concerns of a writing requirement because the writing was not fixed enough and Mallory altered it around the signature, or the signature was invalid for lack of *intent* to sign *this* document. In the face of Clinton's denial that the document is legitimate or that he intended to bind himself to this document, the burden of proof should fall upon Mallory. Mallory

---

58 *See* CHARLES M. HARR & LANCE LIEBMAN, PROPERTY AND LAW 505-07 (1977) (quoting G. BRECKENFELD, COLUMBIA AND THE NEW CITIES 244 (1971)).

59 *See* Massachusetts Electronic Records and Signatures Act (Draft, Apr. 14, 1998), *available at* <http://www.magnet.state.ma.us/itd/legal/mersa.htm>.

60 CASABLANCA (Metro-Goldwyn-Mayer 1942).

61 *See GPO Access - Federal Register (1995-99)* (last modified Apr. 27, 1999) <http://www.access.gpo.gov/su_docs/aces/aces140.html>.

could not prove that Clinton or an authorized party placed the signature on the document and her claim would fail even though Clinton could not prove that Mallory forged the document. An electronic signature law would only buttress that result.

This situation highlights a key consideration in the drafting of digital signature laws: that any formalities laid out therein not disturb rules on the validity of other signatures (including situations such as the one above, of electronic signatures adequately cognizable by existing law). The statute mentioned above should have been unnecessary in this case, only changing the result where existing doctrine does not adequately address the problem. The statute also provides much desired certainty, a kind of insurance against courts that improperly extend existing rules. It may be most desirable to bring informal electronic signatures on par with informal written signatures in that they may be valid, but once the document's integrity or the signer's intent to be bound are placed in issue, they are presumed not to be.

C. *Treatment of Secure Signatures: Evidentiary Presumptions and Proactive Incentives*

While the initial goal of digital signature legislation is to place electronic instruments on par with written ones, certified digital (cryptographic) signatures offer a level of security above that of the average written signature standing alone. It has been suggested by some[62] that a cryptographic signature[63] is most directly analogous to a notarized signature. Admittedly, in both cases an entity licensed for its integrity by the state government has verified the signer's identity. However, in a notarization, the notary's seal indicates that the government-licensed agent verified the signer's identity at the time of the signing and witnessed the act itself. With a cryptographic signature, all we know is that the signer's identity was verified at some time prior to the signing. Even if the certificate authority keeps a database of revoked, expired, or compromised certificates and keys, it is only a comfort if the key's true owner knows the key has been compromised, has reported this to the authority's database, and that database is searchable in real

---

62 *See* NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, UNIFORM ELECTRONIC TRANSACTIONS ACT § 110 (Mar. 19, 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta399.htm>.

63 Note that this similarity to notarized documents would apply only in a full public key infrastructure, where an authority ultimately traceable and accountable to the government (likely licensed by a governmental entity) signs a certificate, and not to PGP's web of trust system, because there public keys are signed only by other individuals.

time.[64] In actuality, the signature is analogous to the previous example of a check attested to by a grocery store clerk after successfully checking the signer's identification. Like the digital signature, a governmental agency (in this case the DMV) has verified the information at the time of the driver's license issuance, but the printed address and possibly even vital statistics and appearance could have changed since then. Thus, a statute giving the effect of a notarization to a digital signature would violate the principle that the legal protection accorded electronic signatures should be no greater than the reliability actually offered by the signature technology.

Some proposals simply state that "nothing in this law precludes any symbol from being a valid signature under applicable law."[65] Additionally, these proposals might state that where the law requires a signature, a digital signature will suffice if it follows specified formal requirements.[66] Thus, no additional validity is conveyed except where all formal requirements are met. Such a proposal therefore ignores the issue of less formal electronic signatures that, to be placed equal with written instruments, should be presumed valid until the specific instrument's value is contested.[67] In order to avoid this problem, a second approach has been to state the requirements for a signature vaguely, so that either formal or informal signatures may qualify if the prerequisites are met.[68] This approach, however, offers no additional protection to more carefully verified methods of digital signing.[69] A third set of laws takes a two-tiered approach.[70] Informal signatures cannot be inval-

---

64 *See, e.g.*, "Scoville v. Safdar" hypothetical, text accompanying note 80.

65 UTAH CODE ANN. § 46-3-401(1) (1998).

66 *See id.* § 46-3-401(2).

67 Again, arguably this may be achieved through current law and is desirable mainly for consistency's sake.

68 *See* CAL. GOV'T CODE § 16.5 (West 1997).

69 This has been a major issue for the drafters of the National Conference of Commissioners on Uniform State Laws' Uniform Electronic Transactions Act. After deciding to state the requirements for an upper level of protection in a generic, technology-neutral fashion, the drafters felt that providing benefits meant for secure signatures might inappropriately grant protection to signatures not in fact so secure. They decided to delete their evidentiary presumptions, and left the issue of the effect of a signing subject to proof under other law. *See* NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, UNIFORM ELECTRONIC TRANSACTIONS ACT (Mar. 19, 1999 Draft) § 108, *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta399.htm> [hereinafter UETA Mar. 1999 Draft]; Memorandum from Ben Beard, Reporter to the Uniform Electronic Transactions Act Drafting Committee and Observers (Nov. 25, 1997), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/etam1197.htm> [hereinafter UETA Nov. 1997 Draft Reporter's Memorandum]; *see also infra* text accompanying notes 112-13 (discussing technology-neutrality).

70 *See* Electronic Commerce Security Act, 1998 Ill. Legis. Serv. P.A. 90-759 (West) (codified at 5 ILL. COMP. STAT. 175/1-101).

idated solely because they are in digital format; rather, they are still subject to proof of the intent to sign, as discussed above.[71] In these models, signatures meeting additional formal requirements are entitled *ab initio* to an upper tier of protection, such as the rebuttable presumption that: (1) the purported signatory or an authorized agent was the one to sign the document; (2) that the signer intended to be bound; (3) that the message has not been altered, and so forth.[72] This last approach, while more complex, is the best alternative for linking the legal value of signatures to the actual integrity of the method used.

Since offering such top tier protections goes beyond giving electronic signatures the same force as paper ones, the true motivation must be to provide incentives so that secure practices will become the norm early in the age of e-commerce. The current situation involving electronic transactions suggests that more secure practices are needed, but that the market may not provide them on its own. The use of encryption in transmitting payment information, combined with the fifty dollar liability limit for fraudulent use, has eased consumers' fears about interception of their credit card data by malicious third parties.[73] Merchants are still in a difficult spot, however, because they bear the full losses from fraud when the signature on a card cannot be verified.[74] Moreover, the rate of card fraud on the Internet is substantially higher than in the real world, particularly for software and other products that can be delivered instantaneously and electronically.[75] While the rate of fraud has decreased, many of the primary methods of combating it, such as black-listing suspected crooks and using data profiling to identify those purchasers likely to be thieves, raise serious questions about discrimination and the privacy of personal data.[76] Even so, consumers' satisfaction with on-line security and

---

71 *See id.*

72 *See id.*

73 *See* Saul Hansell, *Internet Merchants Try to Fight Fraud in Software Purchases*, N.Y. TIMES, Nov. 17, 1997, at D1.

74 *See id.*

75 *See id.* C|net's Buydirect.com reports a fraud rate with periods as high as 20% during 1997. *See id.*

76 *See id.* Privacy advocates have long decried the increasing collection and dissemination of personal information by commercial entities. Moreover, the discriminatory effects of scattershot profiling may not even be legally redressable. Unlike the profiling of air travelers, or the widely publicized 1997 incident involving Eddie Bauer Inc. (in which a clothing store was sued for racial discrimination for confiscating a t-shirt from a black teenager who was singled out and asked for but was unable to produce a receipt for the shirt he had bought the day before), *see* Ruben Castaneda & Jackie Spinner, *Teens Awarded $1 Million in Bauer Case*, WASH. POST, Oct. 10, 1997, at A1, the factors profiled in on-line commerce probably do not involve suspect classes. The famous *New Yorker* cartoon, "On the Internet, nobody knows you're a dog," is applicable, although they do know that you are

reluctance to use more complicated procedures may stifle merchants' willingness to replace ordinary, unauthenticated credit card orders with more secure protocols, such as the VISA/MasterCard Secure Electronic Transactions ("SET") system.[77] While the market should eventually dictate the adoption of such systems if fraud is high enough,[78] legislation promoting more secure methods could stimulate greater market efficiency while reducing the need for profiling and black lists. The correction of such deficiencies through the encouragement of more secure authentication methods is perhaps the most compelling argument for action by legislation, as legislation is arguably the most appropriate avenue for enacting such proactive policy incentives.

The force of protection provided to digital signatures is often established through statutory evidentiary presumptions. These presumptions are not insurmountable, but merely clarify that the validity of the signature is presumed unless the party seeking to show that it is not valid can meet a burden of proof[79] to rebut the presumption. Unlike informal signatures, the challenger would have to prove the forgery affirmatively.

Some digital signature statutes and regulations provide no evidentiary presumptions at all. In a jurisdiction providing no presumptions, a digital signature is ideally on the same footing as a paper signature. One argument in favor of presumptions is that, in practice, paper documents and ink signatures enjoy the functional equivalent of a presumption because threshold requirements for admissibility are so low. Furthermore, the theoretical ease of forgery in the electronic realm makes it much easier to charge that forgery has occurred. Perhaps evidentiary presumptions are then justified to eliminate this disparity where, as with cryptographic digital signatures, such forgery is actually unlikely.

---

ordering business software late at night, or that you are ordering from Israel or South America, which are indications of an increased probability of fraud. *See id.*; *see also* Peter Steiner, NEW YORKER, July 5, 1993, at 61 (cartoon), *available at* <http://www.cartoonbank.com/images/22230_hi.gif>.

77 *See* Saul Hansell, *New Security System for Internet Purchases Has Its Doubters*, N.Y. TIMES, Nov. 24, 1997, at D1.

78 *See id.* (reporting that VISA will offer merchants some relief from fraud liability if they use SET).

79 A previous Uniform Electronic Transactions Act ("UETA") draft imposed only a burden of production to burst the presumption, but other discussion has not been so specific, suggesting perhaps, that the burden of *persuasion* might be imposed. *See* NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, UNIFORM ELECTRONIC TRANSACTIONS ACT (March 23, 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta398.htm>.

D. *Hypothetical Transactions*

The following hypothetical situations are offered in order to place in context the operation of the common law and various digital signature laws. In some cases, there is a "right" answer as to what result should occur when the document is challenged under statutory writing or signature requirements. In other cases, the expected outcome depends on policy decisions which may be in some debate. The function of these examples is not only to point out where statutes have clear deficiencies or where they plainly overreach, but also to identify controversial decisions of policy. Some of these situations have already been introduced.

> *Mallory v. William J. Clinton* - Mallory goes to court with the document in Exhibit Five seeking damages for being denied the job purportedly offered in the document. She says she received the document electronically and has the e-mail message in which the document was included (but has no personal knowledge and offers no witnesses to prove that Clinton actually signed this document). The header information appears to say that the message came from an e-mail address, which Clinton admits is his. The parties stipulate that this is Clinton's signature, generated from an electronic file he sometimes uses to sign electronic messages, including some personal letters. There are some messages with this electronic signature stored in public sites on the Internet. Clinton insists that Mallory composed the message herself, pasted on Clinton's electronic signature, and falsified the addressing information on the e-mail message.

As discussed above, the document is facially valid but should be excluded from evidence because once Clinton has placed his intent to sign the document in issue, Mallory should be required to prove that Clinton intended to sign the document. If Clinton admits to signing the document (i.e., he meant to offer Mallory the job), another party (e.g., a competitor entitled to the job if the letter had never existed), should not be able to challenge the signature solely on the basis that it is electronic.

> *Scoville v. Safdar* - Scoville seeks to enforce the agreement in the message in Exhibit Four, which bears Safdar's cryptographic signature. Assume that Safdar's key was certified by Trent's Certification, a licensed authority. Scoville is ready to pay the license fee, but Safdar refuses to send the registration codes. The software package with which the signature was created confirms that the signature was technically valid and made using Safdar's private key. Also, Scoville relied on the message, and turned down a limited-time offer on comparable software (meaning he

> would have to pay $5000 more for that software than during the special offer period). First, what if Safdar says he did not realize what this cryptography stuff is all about, and says he may have activated the program to sign the message, but had no idea he was binding himself to the message? Second, what if Safdar says he didn't send the message? Instead, he claims to have discovered a week later that his estranged lover, Mallory, knew the passphrase to his private key (which was a quote from *The Road Ahead*,[80] underlined and labeled "crypto key" in Safdar's dog-eared copy, which Mallory once borrowed without asking). Safdar claims that Mallory sent Scoville the message (from the e-mail address she used to share with Safdar) accepting the offer to license MindWidget for $10,000 less than the usual price, in order to ruin Safdar's business out of spite.

In the first instance, Safdar should clearly be liable, because if this were a paper signature, Safdar would be negligent in signing his name without knowing the consequences, and the same should hold true here. In the second example, assuming that the digital signature is valid, it should be difficult for Safdar to deny the signature; we would want a presumption that he signed it. Safdar would be required to prove that he did not sign it by offering evidence of Mallory's knowledge of the key. Additionally, Safdar's underlining of the passphrase would be questioned as to whether it was consistent with his burden of care in maintaining the secrecy of his key, because if he was negligent in guarding his key, he could be held liable. There is also the question of who should have the burden of proving reasonable care or lack thereof. Since Safdar is in a much better position to know, and he had the burden of disproving the signature's presumed validity in the first place, he should bear the burden.

> *In re Estate of Alice* - Alice recently died. Bob produces an electronic document from Alice's hard drive. It is a will leaving $100,000 of stock in various Internet companies to Bob. It was signed two months before Alice's death with Alice's private key, which was certified by Trent's Certification. The records of Trent's Certification say that Alice came last winter to their branch office in the front of the local natural foods market, showed her photo license and her passport, and was issued a brand new private key corresponding to a public key that Trent signed and certified. Carol, however, produces a paper will dated three years ago, and acknowledged by Alice before the requisite witnesses, which leaves her entire estate to Carol.

---

[80] BILL GATES, THE ROAD AHEAD (1995).

> Carol challenges the electronic will. Would the situation change, from a policy standpoint, if two witnesses watched Alice sign the electronic will with her private key, verified the signature cryptographically themselves, and then each signed the document (including Alice's signature) themselves with their own certified keys? What if one witness is prepared to testify in court that he did in fact sign his own signature and the person who signed the other signature was the person named in that signature?

Several drafting committees (e.g., NCCUSL and the Illinois legislature) have suggested that wills should be exempted from statutes validating digital signatures.[81] However, this example highlights that the digital signing of the will is not what presents a problem (or, likewise, in attempting to make a digital notarization). The certification on a signature verifies that, *at one time*, Alice was the only person who controlled the key. It probably also gives her a duty to report if the key is ever compromised. However, her exclusive control of the key is not affirmatively ascertained at the time of the will's signing. Therefore, the uncertainty stems from the witness requirement for will signing, *not* the writing or signature requirements. If that is the case, should not a will digitally signed with witnesses present be sufficient? Admittedly, this leaves open the charge that the witnesses were using other people's compromised keys, complicit in a fraud by Bob to manufacture the document. Even this concern should be satisfied if the purported witness legally authenticates his signature during an in-court testimony.

IV. Cases on Electronic Signatures: The Picture Without Legislation

A. *The Need for Precedential Analysis*

Efforts to draft digital signature, electronic record, or certificate authority legislation have consistently been predicated on the need to prevent formalistic judges from incorrectly invalidating digital signings. This would yield incorrect results in the examples of Mallory v. Clinton and Scoville v. Safdar (where Clinton and Safdar admit intentionally signing the document). Such judges might prefer the simple calculus that, "a writing is a writing" and a signature means paper and ink, perhaps out of ignorance. Such judges might also be uncomfortable with the fact that properly exe-

---

81 *See* UETA Mar. 1999 Draft, *supra* note 69, § 103(b)(1); 5 Ill. Comp. Stat. 175/5-120(c)).

cuted digital signatures can satisfy all the underlying concerns for document integrity, authenticity, and the signer's intent to bind herself. Such concerns on the part of the drafters of digital signature legislation often result in conclusions that electronic commerce "is currently being conducted amid legal uncertainty regarding the validity and efficacy of the electronic records and documents being used to evidence the commercial transactions and relationships being created."[82] This uncertainty is contradictory to the conclusion of commentators who, looking literally at writing and signature requirements, have suggested that "[i]t is now necessary to repeal, change, or at least reinterpret many writing and signing requirements, as they retard legitimate implementation of electronic commerce."[83] Moreover, commentators seem equally willing to acknowledge that courts have generally been sensitive to changing technology, insofar as they have been willing in the past to apply the spirit of the writing requirement, rather than formally adhering to its literal dictates.[84]

Amidst such conclusory assertions that the status of the law is uncertain and, therefore, digital signature legislation is necessary, the following is an attempt to analyze standing precedent and, where necessary, analogize decisions involving other technologies to the question of electronic writings and signatures. Such an analytical underpinning is crucial to the credibility of assertions that legislation is necessary.

---

[82] UETA Aug. 1997 Draft Reporter's Memorandum, *supra* note 43; *see also* Michael D. Wims, *History and Current Status of the Utah Act* ¶¶ 11, 19 available at <http://www.commerce.state.ut.us/web/commerce/digsig/dsintro.htm> ("Current rules for recognizing valid signatures, satisfying writing requirements, admitting documents into evidence, determining what constitutes an original document, and similar formal requirements often do not clearly address documents or records in computer form. People today face some uncertainty in legally relying on computer-based information . . . . [I]n the case of digital signature technology, waiting for case law to evolve would leave commerce in a period of uncertainty."); 5 ILL. COMP. STAT. 175/1-105) ("[The purposes of Act is to] facilitate and promote electronic commerce, by eliminating barriers resulting from uncertainties over writing and signature requirements, and promoting the development of the legal and business infrastructure necessary to implement secure electronic commerce."); Geanne Rosenberg, *Legal Uncertainty Clouds Status of Contracts on Internet*, N.Y. TIMES, July 7, 1997, at D3.

[83] WRIGHT, *supra* note 46, § 16.1. This comment also suggests, however, the additional purpose discussed with regard to evidentiary presumptions for secure signatures, namely to provide proactive incentives for commerce, rather than merely to remove barriers. *See supra* Part III.C.

[84] *See* JULIAN S. MILLSTEIN ET AL., DOING BUSINESS ON THE INTERNET: FORMS AND ANALYSIS § 8.04[4][b] (1997) ("Over the years, interpretation of the term 'writing' has developed in response to new communications technologies. The introduction of the telegram, the telex, and the facsimile . . . have generally not prevented courts from finding that sufficient writings existed for purposes of the Statute of Frauds."); WRIGHT, *supra* note 46, § 16.5 ("As a practical matter, the statute of frauds' writing and signing clauses are almost illusory barriers to the enforcement of obligations.").

B. *Confusion? What Confusion? The Lack of Precedent Involving Secure Authentication*

With each new item of commentary addressing the treatment of electronic records and signatures, authors continue to agree that no case has yet dealt with a challenge to the validity of cryptographically signed documents.[85] This holds true through the present.[86] Courts are not unanimous, but are generally supportive of writings and signatures in other media involving electronic reproduction (facsimile,[87] telegraph,[88] or telex[89]) or, as it relates to the signature requirement, mechanical reproduction by typewriter.[90] It would be easy to conclude that, since these media are much less secure and involve less effort on the part of the author, cryptographically signed electronic documents are bound to be accepted uniformly as writings with signatures. The cases, however, generally hinge on the question of the signer's intent.[91] Where challenges to a document have been successful, the signer has admitted to making the marks or symbols in question on the specific document, but has asserted that they were made for another purpose, one that falls short of intention to be bound.[92] On the other hand,

---

85 *See* WRIGHT, *supra* note 46, § 16.4.5 ("No reported lawsuit has examined whether a purely electronic message satisfies the statute of frauds."); MILLSTEIN, *supra* note 84, § 8.04[4][a] ("No court has yet addressed the enforceability of purely electronic contracts under the Statute of Frauds."); Christy Tinnes, *Digital Signatures Come to South Carolina: The Proposed Digital Signature Act of 1997*, 48 S.C. L. REV. 427, 434 (1997) ("Currently, no case law specifically supports a digital signature as binding. The closest the courts have come to dealing with electronic signatures have [sic] been cases concerning electronic documents such as facsimiles . . . telexes, telegrams and computer verifications."). Since the publication of these texts, some case law has emerged on purely electronic data, but none involved cryptography or other methods of verification. *See* discussion this Part & *infra* Part IV.C.

86 Search of Westlaw, ALLCASES file (Feb. 9, 1998, updated May 18, 1999) (search for "(sign or signature) [in the same sentence as] (digital* or electronic*)" produced no case disputing a cryptographically authenticated document as written or signed).

87 *See* Bazak Int'l Corp. v. Mast Indus., Inc., 535 N.E.2d 633 (N.Y. 1989) (assuming without deciding that fax was a writing under U.C.C. § 2-201); People v. Guzman, 581 N.Y.S.2d 117, 120 (N.Y. Crim. Ct. 1992) (noting that a fax is acceptable under a requirement of a writing, signed and notarized, so long as the original is retained and made available on request).

88 *See* Howley v. Whipple, 48 N.H. 487, 488 (1869).

89 *See* Joseph Denunzio Fruit Co. v. Crane, 79 F. Supp. 117 (S.D. Cal. 1948). *But see* Pike Indus., Inc. v. Middlebury Assoc., 398 A.2d 280 (Vt. 1979) (holding telegram not allowed under Statute of Frauds – the sole U.S. case to so hold).

90 *See* Watson v. Tom Growney Equip., Inc., 721 P.2d 1302 (N.M. 1986).

91 *See* Hillstrom v. Gosnay, 614 P.2d 466 (Mont. 1980) (holding that telegram stating "PLEASE CONSIDER THIS MY ACCEPTANCE" and ending in (typed) name satisfied signature requirement because author thereby intended to authenticate the document).

92 *See, e.g.,* Parma Tile Mosaic & Marble Co. v. Estate of Short, 663 N.E.2d 633 (N.Y. 1996) (deciding whether automated identifier including company at the top of faxed pages "subscribed" document for statute of frauds purposes; despite intention of programming fax machine header, and intention that header *identify* document to recipient, held inadequate because there was no intent to authenticate the contents of the specific document). This case would be analogous if a party asserted that the name and address in the

in some cases even attacks of the kind labeled above as "purely formalistic" (where both the fact of signing and the intent to sign are admitted by the purported signer) have been successful when dealing with purely electronic media.[93] These cases are worth examining, as they indicate the confusion of the courts and their inability to analogize to electronic media in a manner consistent with trends in other media.

C. *Successful Formalistic Attacks Involving Purely Electronic Media*

In 1997, the Tenth Circuit refused to hold that a computer form constituted a writing under the bankruptcy code.[94] The debtors had phoned the bank and each individually provided their financial information, which the bank employee entered into a computer. The employee then read the information back and asked them to verify the record, which they admitted to doing, although at no time did they sign or see the record. The debtors successfully argued that the statement was not a writing.[95]

In *Walgreen Co. v. Wisconsin Pharmacy Examining Board*,[96] the drugstore chain Walgreens was accused of violating the state law requiring "a written or oral order by a [physician] for a drug" prior to the dispensation of prescription medicine.[97] Written orders required the doctor's signature.[98] Walgreens had set up an experimental program whereby physicians would e-mail prescriptions to

---

"From:" field of an e-mail, or in an automatically generated "signature" on the bottom of an e-mail for identification purposes constituted a legally binding signature. This misses, therefore, the more controversial question of more individualized signings.

93 *See* Bellco First Fed. Credit Union v. Kaspar (*In re* Kaspar), 125 F.3d 1358 (10th Cir. 1997); Walgreen Co. v. Wisconsin Pharmacy Examining Bd., No. 97-1513, 1998 WL 65551 (Wis. Ct. App. Feb. 19, 1998). *But see* People v. Perry, 605 N.Y.S.2d 790, 794 (N.Y. App. Div. 1993) (involving a criminal statute prohibiting "offering a false instrument for filing," where fraudulent Medicaid claims submitted on floppy disks were held to be writings under a statute that defined a writing as written or printed matter "or the equivalent thereof").

94 *See Kaspar*, 125 F.3d 1358.

95 *See id.* It is possible to read this case as a simple, blatant attempt by the bank to evade the law. Significantly, however, the statute in question required merely a writing that the debtors *caused to be made*, which in turn required either that they wrote it themselves, that they *signed it*, or that someone else wrote it and they *adopted* and used it. Therefore, the court should have focused on the writing's electronic form as entered, as if the debtors had been sitting across the desk. However, the court seemed to focus on the communication of information to the person who entered it, where this should have been acceptable so long as the debtors had successfully adopted the record: "Can it be said any plainer? A written statement of financial condition does not mean an oral statement converted into an electronic format." *Id.* As the validity of the "writing" should have depended on whether there was a signing or an adoption of the record, this case is also an excellent example of the merger of writing and signature requirements.

96 No. 97-1513, 1998 WL 65551 at *1 (Wis. Ct. App. Feb. 19, 1998).

97 *See id.*

98 *See id.*

the pharmacy. The court avoided the question of whether the e-mail contained a signature by saying it was "more reasonable" to liken the e-mail to an oral telephone authorization (a category that had been previously held to include fax transmissions) which, by statute, did not require a signature.[99] Here, despite the textual nature of the message, and despite the fact that the court ultimately validated the authorization, the court decided that the e-mail did not constitute a "writing" (and therefore the textual affirmation thereon was not a "signature").[100]

These cases suggest that the status of electronic communications as writings has yet to be settled. The *Walgreen* court focused on the transmission of the data over phone lines (like a fax or an oral call),[101] the *Kaspar* court seems to have been distracted by the intervening phone call, as opposed to whether or not the computer data was fixed,[102] and the court in *Perry*, it has been suggested, was overly focused on the physicality of the floppy disks transferred.[103] While these cases hint of confusion to come regarding electronic records, a more straightforward case of electronic communications in contractual transactions is necessary before any truly pertinent observation can be made.

As was discussed above, whether the document is cryptographically signed or not may become significant in rarer cases where not only the signer's intent to be bound is at issue, but also more fundamental questions — like whether the document has been forged or altered — are at issue. In the hypothetical of Mallory's employment offer from President Clinton, the courts in *Parma Tile* or *Hillstrom* might have rightly disallowed the document by focusing on the signer's intent and by shifting the burden to Mallory to prove the document's authenticity.[104] However, the *Kaspar* court,

---

99 *See id.* at *4.

100 *See id.* Of course, this statute, since it contained an alternate provision for the validity of an oral authentication, was unlike normal writing requirements, so it might conceivably have led to a different holding on the writing question had the alternative not been present.

101 *See id.*

102 *See* Bellco First Fed. Credit Union v. Kaspar (*In re* Kaspar), 125 F.3d 1358 (10th Cir. 1997). Insofar as the writing requirement is concerned with the fixation of the text, case law interpreting the fixation requirement in copyright law may be analogous, although commentators have suggested that courts have badly misinterpreted the requirement as in some situations under *MAI v. Peak*, 991 F.2d 511 (9th Cir. 1993). *See* Kristen J. Mathews, *Misunderstanding RAM: Digital Embodiments and Copyright*, 1997 B.C. INTELL. PROP. & TECH. F. 041501 (Apr. 15, 1997) <http://www.bc.edu/iptf>.

103 *See* People v. Perry, 605 N.Y.S.2d 790, 795 (N.Y. App. Div. 1993); WRIGHT, *supra* note 46, § 16.4.5 (supplement page S-16.2) (suggesting that the court had thought that the state agency kept the very same disks the defendants submitted and made the printouts from those, rather than from a copy archived in a central file server).

104 *See* Parma Tile Mosaic & Marble Co. v. Estate of Short, 663 N.E.2d 633 (N.Y. 1996).

given its disregard for the fact that the debtors intentionally acknowledged the information that was read back to them, might have gone the opposite way.[105] One can only hope that these courts would see a cryptographic signature as strong evidence of a signer's intent, but again, given the *Kaspar* and *Walgreen* courts' disregard of the affirmant's intent to authenticate or adopt the communications, one can hardly be sure.[106] Given this uncertainty, cases holding earlier electronic media to be writings, or holding that marks made in manifestation of intent are signatures may be insufficient to extrapolate a rule that might be applied to cryptographically signed documents.

V. Subsidiary Concerns in Certificate Authority Legislation

A. *Licensure, Certification, or Registration of Certificate Authorities*

The first digital signature statute passed, the Utah Digital Signature Act[107] (and likewise several successors modeled on it), enacted a comprehensive regulatory scheme for the use of digital signatures and certificate authorities. Whether or not to enact such a comprehensive statute is an important policy question, and even states with such comprehensive statutes have recognized that appropriate action may also be possible through regulation rather than legislation.[108] Indeed, leaving the details to regulatory specification may be more appropriate for legislatures that are unenthusiastic about the degree of legislative involvement that may be necessary as digital signature law and electronic commerce evolve.[109] When legislatures allocate the responsibility between themselves and their administrative agencies for keeping their law up to date, they must pragmatically consider their own level of commitment, and recognize that digital signature law will need to be revised as the industry matures.

States must decide the extent to which they intend to regulate the functioning of certificate authorities. There are three important and crucially distinct considerations: first, whether legislation is necessary to ensure or promote the validity and admissibility of electronic signatures; second, whether a public key infrastructure is necessary for digital signatures to function reliably; and third, if so, whether the regulation of certificate authorities is necessary? The

105 *See Kaspar*, 125 F.3d 1358.
106 *See id.*; *see also* Walgreen Co. v. Wis. Pharmacy Examining Bd., 1998 WL 65551 at *4 (Wis. Ct. App. Feb. 19, 1998).
107 Utah Code Ann. § 46-3 (1996).
108 *See* Wims, *infra* note 82.
109 *See id.*

enactment of more limited statutes without regulation of certificate authorities is not merely an interim or halfway measure; public key infrastructures ("PKIs") may simply not be necessary. Contrarily, market-driven demand for certificate authority services and cryptographic signatures may generate an independent need for the regulation of authorities in the interest of consumer protection. Drafting groups have come to a variety of decisions on the regulation of certificate authorities. These choices have ranged from comprehensive licensing schemes for certificate authorities, to intermediary measures (such as voluntary licensure or registration programs, or deferring to federal or industry accreditation groups – many as yet unnamed and uncreated), to leaving authorities practically unregulated.[110]

On a substantive level, decisions on the licensure or accreditation of authorities include requirements that authorities hire reliable and scrupulous personnel,[111] maintain proper records, and use "certification practice statements" to define the value and degree of verification undertaken in issuing certificates. In addition, states might require agents for service of process in the case of lawsuits, or contingency arrangements for the proper handling of certificates should an authority cease operations. The most critical requirement is, however, the financial reserve carried by certificate authorities. The potential liability of an authority for accidentally or negligently certifying an untrue statement could be enormous, depending on the size of the transaction in which a party relied on the certified facts. Without regulation, there is a danger that small start-up authorities might not carry enough insurance or have the financial resources to meet their liabilities.

B. *Technology-neutrality*

At present, the most reliable form of electronic signature technology, and the only form of signature approaching any degree of wide adoption, uses asymmetric cryptographic keys and certificates. Many drafting groups are afraid of inadvertently giving legal pro-

110 If a comprehensive and well respected national industry licensing body were to develop, sufficient legal compatibility may be achievable without federal action. While uniform law bodies can promulgate state laws that address the legal validity of signatures, such uniform laws do not mandate state administrative bureaucracies, such as would be dictated by licensing and accreditation needs. Therefore, in the absence of applicable industry standards, the federal government could eventually play a useful role in regulating certificate authorities.

111 In the Scoville v. Safdar example, where Mallory supposedly signed the message with Safdar's key, imagine if this appearance had been created because Mallory had bribed one of Trent's employees into issuing *her* a certificate in Safdar's name.

tection in instances where the technology does not provide a commensurate level of security. Therefore, several states have chosen to make their digital signature laws apply specifically to cryptographic signatures, defining a "digital signature" as the transformation of a message using asymmetric cryptography.[112] Technology-specific laws, however, cannot anticipate the development of other methods, which might offer equal levels of security. Deliberately writing inflexible laws in this case may erect inappropriate barriers to the development of new and effective digital authentication techniques. Drafters of technology-specific laws wager that what they sacrifice in flexibility will be made up with reassurance that they are not inadvertently providing legal advantages to technologies that do not warrant them.

Increasingly, states have opted for technology-neutral laws which do not mention or prefer specific methods and state their requirements generically instead. Some of these laws achieve technology-neutrality by decreasing the level of detail of the law in general. A most basic law might simply provide that a digital signature is valid only where "it is unique to the person using it[,] it is capable of verification[,] it is under the sole control of the person using it[, and] it is linked to data in such a manner that if the data are changed, the digital signature is invalidated."[113] There is a fine line to walk, however, to avoid granting excessive protection to less secure signatures, particularly where the statute provides for evidentiary presumptions. The most prudent compromise is that proposals shy away from technology-specific terms, but enumerate the security requirements necessary for the granting of legal protection with as much specificity as possible.

C. *The Validity of Signatures Based on Preexisting Contracts*

Generally, digital signature laws are aimed at parties whose relationship does not arise in the context of an already existing contract, because in such a case the contract may already provide for the validity of electronic signatures. However, many important payment systems for electronic commerce will provide a contractual basis for the transaction, just as credit card agreements provide a contractual framework for transactions between otherwise unassociated parties. In the Secure Electronic Transaction ("SET") system, both parties have contractual privity with the certificate issuer,

---

112 *See* UTAH CODE ANN. § 46-3-103(10); 5 ILL. COMP. STAT. 175/5-105) (making top tier "digital signatures" technology-specific, while informal "electronic signatures" are technology-neutral).

113 CAL. GOV'T CODE § 16.5 (West 1997).

just as both the merchant and the buyer in a credit card purchase have contractual arrangements with their banks, which in turn have contractual arrangements with Visa or MasterCard.[114] Thus, the parties in the SET system already know, by virtue of the buyer's presentation of a SET account, and the seller's ability to accept that credit, that the SET system has vouched for the fact that the buyer will pay up (and the seller will deliver the goods).[115] Therefore, the full security of a certificate from a certificate authority regulated by state or federal governments may not be necessary.

If a state law, however, says that a digital signature is valid (only) if *A*, *B*, and *C* terms are met, the law might invalidate already evolving contractual mechanisms using bases for security other than *A*, *B*, and *C*. This has been a chief concern of entities, such as Visa, which are developing contractual payment models like SET.[116] Although a law's deference to preexisting contracts has the biggest impact on large payment systems, the question is really one of contractual freedom and honoring the mutual intent of the parties to be bound by signatures in the form they choose. Therefore, a provision allowing some of a law's requirements to be varied by agreement would be advisable.

D. *Limits on Liability*

When digitally certified information is false, most disputes over liability will occur between the authority and the third party relying on the certificate's accuracy, not between the authority and its customer. Therefore, many drafters have considered limiting the tort liability of certificate authorities. Once the validity of certificates and signatures is established, it can and should be left to the market and to courts and juries to determine the liability of authorities. This will result in a valuation and assessment of responsibility more closely compatible with existing principles of liability in contract and common law.

---

114 *See* Saul Hansell, *New Security System for Internet Purchases Has Its Doubters*, N.Y. TIMES, Nov. 24, 1997, at D1.

115 *See id.*

116 *See Federal Role in Electronic Authentication: Hearings before the Subcomm. on Domestic and Int'l Monetary Policy of the House Comm. on Banking and Fin. Serv.*, 105th Cong. (July 9, 1997) (statement of Andrew Konstantaras, Vice President and Counsel, Visa Int'l Serv. Assoc.), *available at* <http://www.house.gov/banking/7997kons.htm>. The flexibility to agree (as in the SET agreement) to the validity of less secure signatures or payment methods may be provided where laws say that digital signatures in general are valid if the law specifically allows variation by agreement, or may be subsumed by passages clarifying validity where the parties intend to be bound. The concern here, however, is not for allowing the validity of certain informal signatures, but for keeping the law from interfering with already valid contractual arrangements.

The arguments for statutory specification of liability are twofold. First, some have argued that with the picture of authorities' liability so unclear, potential authorities will be reluctant to enter the market.[117] However, while legal impediments to the *acceptance of digital signatures* are undoubtedly holding the market back,[118] it is not clear that *fear of liability exposure* is. On the other hand, the specification of liability may be necessary for the opposite reason: to keep authorities from *avoiding* liability.[119]

If liability for an authority's negligence or willful misconduct is limited or removed, the authority will have little incentive to carry out competently its core business responsibility, the verification of the facts it certifies.[120] In cases where the authority fulfilled its re-

---

117 *See* Froomkin, *supra* note 31, § III.B (1996).

118 Several participants at a 1997 National Institute of Standards and Technology conference on digital signature standards commented on the concreteness of legal obstacles to the widespread use of digital signatures. *See Public Forum on Certificate Authorities and Digital Signatures*, National Institute of Standards and Technology, Gaithersburg, Maryland, July 24, 1997.

119 *See* Froomkin, *supra* note 31, § III.B. At the time of Froomkin's article, standard contracts by certificate authorities disclaimed virtually all liability, including liability for negligence by the authority itself. For an entity that seeks by its very nature to be a trustworthy party, to be allowed to say essentially that it is untrustworthy and nothing it certifies can be relied on, reduces the value of its services to a nullity. It is as if an insurance company offered policies, but said in the fine print that it would refuse to pay any claims. Since then, matters have improved slightly. VeriSign's current Certification Practice Statement ("CPS") includes the representation to reasonably relying parties that, "(i) all information in or incorporated by reference within the certificate, except nonverified subscriber information (NSI), is accurate, and (ii) the [issuing authority] has substantially complied with the CPS when issuing the certificate." *See* VeriSign, Inc., *VeriSign Certification Practice Statement*, § 6.5.2 (version 1.2, May 30, 1997) (visited Feb. 2, 1999) <http://www.verisign.com/repository/CPS/>. However, the CPS still disclaims that:

> EXCEPT AS EXPRESSLY PROVIDED IN THE FOREGOING (CPS Section 11.3),

[which includes that they "warrant and promise . . . to honor the various representations to subscribers and to relying parties presented in CPS Section 6.5"]

> ISSUING AUTHORITIES AND VERISIGN DISCLAIM ALL WARRANTIES AND OBLIGATIONS OF ANY TYPE, INCLUDING ANY WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, *AND ANY WARRANTY OF THE ACCURACY OF INFORMATION PROVIDED, AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE AND LACK OF REASONABLE CARE.*
>
> Except as expressly stated in the foregoing CPS Section 11.3, [issuing authorities] and VeriSign:
>
> - do not warrant the accuracy, authenticity, reliability, completeness, currentness, merchantability, or fitness of any information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of issuing authorities and VeriSign,
> - shall not incur liability for representations of information contained in a certificate, provided the certificate content substantially complies with this CPS.

Id. § 11.4 (italicized emphasis added). VeriSign does offer an enhanced protection plan, but this only protects subscribers (including a subscriber relying on another's VeriSign certificate). *See* VeriSign, Inc., *NetSure*[SM] *Protection Plan – Version 1.0* (June 20, 1997) <http://www.verisign.com/repository/netsure/index.html>.

120 The Utah Act does, however, limit such liability. *See* discussion of the Utah Act, *infra* Part VI.A.1. *See also* UTAH CODE ANN. § 46-3-309(2)(a) (1998).

quirements without negligence or willful misconduct, liability should be connected to the reasonableness of relying on the particular certificate, in light of the security of the verification process. Since the authority is arguably in the best position to assess the diligence of the verification, it may be acceptable to allow the authority to specify the recommended limits of reliance on a given security procedure and limit their liability thereto.[121] As to limits on the types of damage that could be claimed, any reasonable authority knows that others will rely on its certificates. Therefore, from a policy standpoint some level of consequential damages should perhaps be allowed. It may be appropriate here as well, however, to limit such damages to reliance limits set by the authority.

VI. Survey of Current Proposals and Statutes and Their Interrelation

A. *State Statutes*

1. Utah

The Utah Digital Signature Act ("Utah Act"),[122] the nation's first thorough digital signature law, takes a very detailed regulatory approach toward electronic signatures.[123] The law specifically avoids invalidating any other signature, mark or affirmation that would otherwise be considered valid.[124] However, the law is technology-specific because in validating "digital signatures," the law includes only public key cryptographic signatures.[125] Therefore, the legal status of less formal electronic signatures is left just as uncertain as it would be in the law's absence. The Utah Act would offer no clarification either way, for example, in the case of Mallory's electronically signed employment contract from Bill Clinton, regardless of whether Clinton's intention is to deny or affirm its validity.

The Utah Act primarily sets out an elaborate system for the licensure of Certificate Authorities.[126] The Act includes requirements of surety bonds for conducting business,[127] formal require-

---

121 The Utah Act, however, eliminates all liability here. *See* discussion of the Utah Act *infra* Part VI.A.1. *See also* Utah Code Ann. § 46-3-309(2)(b).
122 *See* Utah Code Ann. § 46-3 (1996).
123 *See id.*
124 *See id.* § 46-3-401(2).
125 *See id.* §§ 46-3-401, 46-3-403.
126 *See id.* §§ 46-3-201 to -204, 46-3-302 to -307.
127 *See id.* § 46-3-201.

ments that must be met for a certificate to be valid,[128] and procedures for the revocation of certificates and the dissolution or revocation of licenses of certificate authorities themselves.[129] In addition, the law sets forth specific and extensive presumptions.[130] These presumptions include that: the information in a valid certificate is accurate; the signature is that of the subscriber listed in the certificate; and the signature was affixed with the intent of signing the message.[131]

The least copied provisions of the Utah Act are its tight restrictions on certificate authority liability.[132] For example, where the authority complies with its requirements, it has *no liability* for reliance on a false certificate.[133] Even in cases of negligence or willful misconduct by an authority, liability for reliance on any false information in a certificate is limited to the "reliance limit" of the certificate, set by the certificate authority.[134] Furthermore, damages against an authority are strictly limited to direct, compensatory damages; punitive, lost profits, and pain and suffering damages are all specifically excluded.[135] In short, Utah's law does little to make sure that its certificate authorities are truly the trustworthy institutions which participants in electronic commerce should expect.

While it is a substantial beginning to legal discussion of digital signature legislation, Utah's Act is not an adequate legal solution for two reasons. While predicated on legal uncertainty over electronic signatures, it only relieves that uncertainty for a narrow class of digital signatures. Further, while its regulatory framework could be used to ensure adequate consumer protections and oversight of this nascent service industry, it does not do so. Instead, the Utah Act works like a farmer opening the gate and escorting the fox into the barn yard. The generous releases from liability sanction carelessness in verifying certificates and leave consumers unprotected against companies already prone to abuse the responsibilities that are at the core of their existences.[136]

---

128 *See id.* § 46-3-302.
129 *See id.* §§ 46-3-201 to 204, 46-3-306 to 307 (1996).
130 *See id.* § 46-3-406.
131 *See id.*
132 *See id.* § 46-3-309.
133 *See id.* § 46-3-309(2)(a). This applies whether the certificate was false because its security was compromised (the subscriber has a duty to safeguard the key), or because the subscriber made a misrepresentation which was concealed beyond the authority's duty to confirm.
134 *See id.* § 46-3-309(2)(b).
135 *See id.* § 46-3-309(2)(c).
136 *See* VeriSign, Inc., *VeriSign Certification Practice Statement*, § 6.5.2 (version 1.2, May 30, 1997) <http://www.verisign.com/repository/CPS/>; *see also* Froomkin, *supra* note 31, § III.B.

2. California

Section 16.5 of the California Government Code ("California Act")[137] contains none of the specificity of the Utah Act. It simply provides that a signature has the same force as a manual signature if, and only if:

> It is unique to the person using it.
> It is capable of verification.
> It is under the sole control of the person using it.
> It conforms to regulations adopted by the Secretary of State.[138]

In the summer of 1998, the California Secretary of State issued final regulations in furtherance of section 16.5. Even when these regulations are considered, however, they do not rise to the level of detail of the Utah statute.[139] For example, for a digital signature technology to be declared "acceptable" for the purposes of the statute's protection, it must only be able to create signatures conforming with the statute.[140]

Currently, public key cryptography is such an "acceptable technology," as is signature dynamics.[141] The regulations set out requirements for Certificate Authorities only so far as requiring that they pass performance audits every two years or be approved by an international accreditation body.[142] However, the performance audits are only aimed at seeing that the issued certificates meet regulations which slightly expand on the vague statutory requirements.[143] Most regulations merely describe properties inherent to most basic public key systems.[144] For example, a digital signature is "capable of verification" if (1) the acceptor of the signed document can verify the signature by using the signer's public key to decrypt the message; and (2) the form(s) of identification which were required for the issuance of the certificate are specified.[145]

Most importantly, the California scheme does not involve the

---

137 CAL. GOV'T CODE § 16.5 (West 1997).
138 *Id.* California's legislation only applies to communications or transactions with the state government. However, its model requirements and simple structure are noteworthy in apposition to the Utah Act, and have been widely considered. In some cases they have been adapted and enacted as applying to public and private communications generally. *See, e.g.*, NEB. REV. STAT. § 86-1701 (1998).
139 *See* CAL. CODE REGS. tit. 2, §§ 22000-22005 (1998), *available at* <http://www.ss.ca.gov/digsig/regulations.htm>.
140 *See id.* § 22002.
141 *See id.* § 22003(a)-(b).
142 *See id.* § 22003a.6.C.-D.
143 *See id.*
144 *See id.* § 22003a.2.-5.
145 *See id.* § 22003a.3.

licensure and approval of certificate authorities, except insofar as the state maintains an "Approved List of Certification Authorities," which are those that have passed the audit requirements.[146] The regulations make no requirements for authorities' financial security or the posting of surety bonds. The regulations also create no evidentiary presumptions, although they do state that the subscriber "assumes a duty to exercise reasonable care to retain control" of her private key.[147] Finally, and perhaps most significantly, the regulations do not set liability limits or mention recommended reliance limits for certificates and certificate authorities. The requirements for signature dynamics signatures are similarly elementary.[148]

3. Illinois

While the Utah and California laws provide reference points within which to frame a discussion, subsequent efforts have offered further beneficial refinements. For example, the Illinois Electronic Commerce Security Act ("IECSA" or "Illinois Act"),[149] passed in August, 1998, legitimizes electronic signatures in general, where the signer intends to be bound. Thus, it is open to and enabling of technology and would not interfere with any contractual arrangements for electronic transactions. Additional provisions, however, set up operational requirements for certificate authorities in public key infrastructures.[150]

If a document is signed and can be verified using a security procedure (set out in requirements for public key cryptographic certificates or agreed to by the parties), the signature is considered a "secure electronic signature."[151] These "secure electronic signatures" are then entitled to a higher tier of validity, including evidentiary presumptions, such as the signer's intent to be bound in signing (thus, presumptively satisfying the requirement of intent in the general legitimizing language).[152] The IECSA also contains innovative language that exempts from its coverage instances when applications would be "repugnant" to the context of the statute in question, or clearly inconsistent with the manifest intent of the law-

---

146 *See id.* § 22003a.6.
147 *See id.* § 22003a.4.
148 *See id.* § 22003(b).
149 *See* Electronic Commerce Security Act, 1998 Ill. Legis. Serv. P.A. 90-759 (West) (codified at 5 ILL. COMP. STAT. 175/1-101).
150 *See* 5 ILL. COMP. STAT. 175/15-301 to 320, 175/20-100 to 110.
151 *See id.* 175/10-110.
152 *See id.* 175/10-120, 175/10-130.

making body.[153]

Further, the IECSA sets defaults for the warranties implied to those who rely on the certificate and the level of confirmation the authority has done in issuing the certificate.[154] Both of these defaults may be overridden by policies specifically laid out in the authority's certification practice statement ("CPS").[155] The law also specifies the subscriber's duty to retain control and security over the private key.[156] It allows flexibility in the level of regulatory involvement, specifying that the regulatory agency may impose additional requirements on "secure electronic signatures."[157] The IECSA allows the state to establish a voluntary licensing system, to require that authorities be accredited by independent industry accrediting entities, or to specify criteria for a list of approved authorities.[158] Even beyond its focus on a signer's intent, the IECSA also contains an explicit "variation by agreement" clause to protect the validity of security procedures agreed to by contract.[159] It is noteworthy, finally, that the IECSA was an important source for the draft Uniform Electronic Transactions Act.[160]

The IECSA represents a well-balanced approach to digital signature regulation because its two-tiered system provides for informal electronic signature, while still offering appropriate enhanced protections to encrypted signatures without fear that those protections would later be applied to different, possibly less secure signatures. It avoids many of the pitfalls in earlier proposals, including: (1) unnecessarily affecting contractual systems like SET; (2) affecting wills, land transfers, and other such areas where digital signing may still be inappropriate; and (3) specifying of excessive liability limits. In the upper tier of protection (the so-called "secure electronic signatures") the IECSA is not technology-neutral. This is probably an appropriate choice, particularly at this experimental phase in the development of digital signature laws. The IECSA offers robust legal protections to secure electronic signatures. Given that the true security of other electronic signature methods is somewhat hypothetical, reserving these protections to crypto-

153 *See id.* 175/5-115.
154 *See id.* 175/15-310, 175/15-315.
155 *See id.*
156 *See id.* 175/10-125, 175/20-105 to 110.
157 *See id.* 175/15-105, 175/15-115.
158 *See id.*
159 *See id.* 175/1-110.
160 *See* Memorandum from D. Benjamin Beard, Reporter to the Drafting Committee for Electronic Communications in Contractual Transactions (April 10, 1997), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/ecomemo.htm> [hereinafter UETA Apr. 1997 Draft Reporter's Memorandum].

graphic signatures exclusively is consistent with correlating the legal protection offered with the security of the applicable technology.

4. Massachusetts

Massachusetts has also been preparing legislation that aims to remove legal obstacles to the acceptance of electronic signatures with as little excess complexity as possible. The Massachusetts Electronic Records and Signatures Act ("MERSA")[161] avoids creating a regulatory burden for the state by never mentioning certificate authorities. It does not grant inappropriate protection, for it contains no upper "tier" (or any enhanced protection) for more secure signatures. At its core, the draft adopts and refines the essential core provisions from the UNCITRAL Model Law on Electronic Commerce:

> Section 67. Electronic Records.
> A record may not be denied legal effect, validity, or enforceability solely because it is in the form of an electronic record. If a rule of law requires a record to be in writing, or provides consequences if it is not, an electronic record satisfies that rule of law.
> Section 68. Electronic Signatures.
> A signature may not be denied legal effect, validity or enforceability solely because it is in the form of an electronic signature. If a rule of law requires a signature, or provides consequences in the absence of a signature, an electronic signature satisfies that rule of law.
> Section 69. Admissibility into Evidence.
> In any legal proceeding, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of an electronic record or electronic signature into evidence on the sole ground that it is an electronic record or electronic signature or on the grounds that it is not in its original form or is not an original.[162]

Similarly, "[a] contract between business entities shall not be unenforceable, nor inadmissible in evidence, on the sole ground that the contract is evidenced by an electronic record or that it has

---

161 Massachusetts Electronic Records and Signatures Act secs. 3-4 (Draft, Apr. 14, 1998), *available at* <http://www.magnet.state.ma.us/itd/legal/mersa.htm>. Laws modeled on the Massachusetts draft have already been enacted in some states. *See, e.g.,* KY. REV. STAT. ANN. § 369 (Banks-Baldwin 1998); OKLA. STAT. tit. 15, § 960 (1998). In addition, the drafters of MERSA have been noted for their contribution to the drafting of Senate Bill 761, the Millennium Digital Commerce Act. *See* Spencer Abraham, *The Millennium Digital Commerce Act* (visited Mar. 25, 1999) <http:///www.senate.gov/~abraham/mdcas.html> (statement on bill's introduction).

162 Massachusetts Electronic Records and Signatures Act sec. 4, ch. 30 §§ 67-69.

been signed with an electronic signature."[163]

These provisions would not apply if they are "clearly inconsistent with the purpose of that rule of law," although it is specified that the mere requirement that the record be "signed" or "in writing" does not demonstrate such a purpose.[164] This "repugnancy" clause, as it is known,[165] was adopted by the Illinois Act and considered but rejected by the NCCUSL as a way of effectively limiting the scope of digital signature laws. Theoretically, the language would prevent the laws from reaching wills, trusts, and title documents for interests in real estate, for example, without having exhaustively to list either exclusions or inclusions.[166]

The minimalist nature of the Massachusetts draft makes it more akin to the California approach than to the expansive Illinois and Utah statutes. Among such "thin" digital signature laws, the MERSA is preferable. Unlike the California Act, which declares that digital signatures are valid (and might, by the pregnant negative, imply that something else is less valid), the Massachusetts draft merely removes obstacles to the recognition of signatures.[167] In addition, the repugnancy clause, while perhaps ambiguous, provides an appropriate limitation where the California language, if adopted in a context beyond its scope of communications with state government, may be broader than desired in scope.

B. *Uniform Law Models and Drafts*

1. American Bar Association Digital Signature Guidelines

The American Bar Association Digital Signature Guidelines ("ABA Guidelines") provided an elementary foundation for the development of digital signature legislation.[168] In some respects, however, its status as a formative document is clear. Its consideration of many issues (such as technology-neutrality, legal presumptions, the validity of signatures not meeting its requirements based

---

163 *Id.* sec. 5, ch. 93 § 108.

164 *See id.* sec. 4, ch. 30 § 66; *id.* sec. 5, ch. 93 § 108.

165 A previous version of MERSA excluded constructions that would be "clearly inconsistent with the manifest intent of the lawmaking body or repugnant to the context of the same rule of law." Massachusetts Electronic Records and Signatures Act sec. 3, ch. 30 § 66, sec. 4, ch. 93 § 108 (Draft, Nov. 4, 1997).

166 *See id.* The NCCUSL felt that this approach would, in leaving the determination of repugnancy up to the courts, cause confusion. They therefore opted to specify exclusions. *See* UETA Mar. 1999 Draft, *supra* note 69, § 103(b).

167 *See* Massachusetts Electronic Records and Signatures Act sec. 4, ch. 30 § 67-68.

168 INFORMATION SECURITY COMMITTEE, SECTION OF SCIENCE AND TECHNOLOGY, AMERICAN BAR ASSOC., DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE (Aug. 1, 1996), *available at* <http://www.abanet.org/scitech/ec/isc/dsgfree.html> [hereinafter ABA GUIDELINES].

on intent or the parties' prior agreement, and liability limits) is primitive. The ABA Guidelines were developed in conjunction with the Utah Act by groups with several common members.[169]

The ABA Guidelines define a digital signature very narrowly:

> A transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine (1) whether the transformation was created using the private key that corresponds to the signer's public key, and (2) whether the initial message has been altered since the transformation was made.[170]

Thus, like the Utah law, the ABA Guidelines grant validity only to public key cryptographic systems. Notice that this definition corresponds to that of the higher tier in the Illinois Act.[171] Therefore the ABA Guidelines, like the Utah Act, would not clarify the enforceability of less formal electronic signatures executed with the intention of authenticating the document. The ABA Guidelines might, therefore, pose problems in alternate contractual situations like SET.[172]

The ABA Guidelines' failure to consider the signer's intent in informal signings is mirrored by its failure to consider the signer's intent where the Guidelines *have* been followed. The ABA Guidelines include legal presumptions consistent with those in the Utah or Illinois Acts, with one significant exception.[173] Given a valid digital signature, the ABA Guidelines do not provide the presumption that the signer intended to bind himself as he would with a manual signature.[174] Without presuming the intention to sign (which is

---

169 *See id.*

170 *See id.* § 1.11.

171 *See id.*; *see also* 5 ILL. COMP. STAT. 175/10-105 to 175/10-135 (West 1998).

172 The ABA Guidelines do allow for variation by agreement, but only in the case of "Persons whose duties are prescribed by these Guidelines," in other words, certificate authorities. *See* ABA GUIDELINES, *supra* note 168, § 2.2.

173 *Compare* ABA GUIDELINES, *supra* note 168, § 5.6, *with* UTAH CODE ANN. § 46-3-406(3)(b) (1998), *and* 5 ILL. COMP. STAT. 175/10-120, 175/10-130. As quoted above, the ABA Guidelines' definition of a digital signature also does not include a requirement of intent.

174 Netizens seem determined to assume the informality and confidentiality of their e-mail. At present, users rarely regard an e-mail message, let alone entries on a web form, to be on par with written instruments. In addition, both Netscape/RSA and Qualcomm/PGP ship widely used Internet e-mail client programs to include digital signature capability as a standard feature. Like the first hypothetical example, Safdar v. Scoville, one could imagine a user clicking on the icon to sign a message and dutifully entering his passphrase without realizing the significance, thinking of it as only another "gee-whiz" feature. Anecdotal evidence, for example, from observing the technophile "fight censorship" and "Electronic Commerce and Rights Management" e-mail lists, suggests that people often sign a document to establish their identity, not to avow the contents of their message.

the defining test for a real-world "signature" in many states), a person who relied on that signature might be defeated by the signer's defense that he simply never intended to be bound.

Like the Utah Act, the ABA Guidelines set liability limits on Certification Authorities.[175] Assuming for the sake of argument that liability limits are needed in order to promote the certificate authority industry, the ABA Guidelines take a more reasonable approach than does the Utah Act. The Utah Act eliminates liability for authorities complying with their obligations, but also limits liability at specified "reliance limits" (a concept not mentioned in the ABA Guidelines) for certificate authorities not in compliance.[176] The ABA Guidelines, however, only provide that, "[a] certification authority *that complies with these Guidelines and any applicable law or contract* is not liable for any loss," either of a subscriber or someone who relies on a certificate.[177] Certificate authorities are still fully liable for intentional or negligent failure to comply with their requirements.

While the ABA Guidelines has been superseded in many respects,[178] its commentary offers thorough consideration of many policy issues not adequately discussed in other contexts, with the possible exception of the commentary to the UETA.[179] For this reason, the Guidelines still represent a necessary starting place in understanding digital signature law and certificate authority regulation.

2. United Nations Commission on International Trade Law Model Law on Electronic Commerce

The United Nations Commission on International Trade Law's Model Law on Electronic Commerce ("UNCITRAL"),[180] which has been approved by the General Assembly, is roughly similar in extent to the Massachusetts draft. The UNCITRAL Model makes no mention of cryptography or certificate authorities, and includes no evidentiary presumptions or liability limits, involving

---

175 *See* ABA GUIDELINES, *supra* note 168, § 3.14.

176 *See* UTAH CODE ANN. § 46-3-309(2).

177 ABA GUIDELINES, *supra* note 168, § 3.14 (emphasis added).

178 Again, the subject of liability limits is a notable exception. While the need for them is questionable, the Utah Act's limits are not an improvement over the ABA Guidelines.

179 This Article is, I hope, helpful in partially rectifying this deficiency.

180 *Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law*, G.A. 51/162, U.N. GAOR 6th Comm., 51st Sess., Annex, Agenda Item 148, U.N. Doc. A/RES/51/162 (1997), *available at* <gopher://gopher.un.org/00/ga/recs/51/RES51-EN.162> [hereinafter UNCITRAL Model Law]. As is discussed below, the general, enabling language of the Model Law is in marked contrast to the specificity of the UNCITRAL Draft Uniform Rules on Electronic Signatures.

the use of electronic signatures. It primarily states that information should not be denied legal effect because it is in electronic form, and that requirements of a written form are met by electronic documents if they are accessible for subsequent reference.[181] Similarly, a data message is adequately signed if

> (a) A method is used to identify that person and to indicate that person's approval of the information contained in the data message; and (b) That method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.[182]

The UNCITRAL Model also addresses the status of electronic messages and files, generally. It specifies when an electronic copy is considered valid as an original, as well as requirements for the retention of data, the formation and validity of electronic contracts, the attribution of messages, and the acknowledgment and legal dating of messages.[183] Several of these sections are reproduced in the UETA. The section on attribution provides that an addressee is entitled to rely on the fact that a message is from and authorized by the purported sender if, in verifying the sender's identity, "the addressee properly applied a procedure previously agreed to by the originator for that purpose."[184] Such reliance is also allowed if the message contains (or the sender necessarily had access to) "a method used by the originator to identify data messages as its own."[185] While this might open the door to less secure procedures in some cases, it would certainly justify the reliance of a recipient on a message containing the sender's digital signature.

The UNCITRAL Model probably could not be translated literally into a state digital signature law. Nonetheless, it has made two contributions that have been incorporated in domestic proposals. First, stating that data "should not be denied legal effect because it is in electronic form" forms the heart of the Massachusetts draft.[186] Second, the requirement that security procedures be as "reliable as was appropriate for the purpose" is worth further discussion (even if in the end it might be unworkably subjective) as an alternative to

---

181 *See id.* art. 5-6.
182 *Id.* art. 7.
183 *See id.* arts. 8, 10, 11, 13, 14, 15.
184 *See id.* art. 13 ¶ 3.
185 *Id.*
186 *Compare* UNCITRAL Model Law, *supra* note 180, art. 5, *with* Massachusetts Electronic Records and Signatures Act sec. 3, ch. 30 § 67-68.

rigid tiers of protection.[187]

3. National Conference of Commissioners on Uniform State Laws - Uniform Electronic Transactions Act

The National Conference of Commissioners on Uniform State Laws ("NCCUSL") draft Uniform Electronic Transactions Act ("UETA") represents a major attempt to provide a consistent national framework for the validity of electronic signatures.[188] While detailed about legal requirements for signatures and authentication,[189] the UETA draft is completely technology-neutral, referring to encryption, only rarely, as one valid option among many.[190] The UETA draft attempts wherever possible to be consistent with analogous provisions in the current Uniform Commercial Code.[191] The drafting committee has also worked with the drafters of the proposed Uniform Computer Information Transactions Act, formerly the draft U.C.C. Article 2B, to coordinate the two proposals.[192]

---

187 *See* UNCITRAL Model Law, *supra* note 180, art. 7 ¶ 1(b). This language was incorporated into the Federal Government Paperwork Elimination Act, Omnibus Consolidated Appropriations, H.R. 4328, 105th Cong., Division C, tit. XVII § 1703(b)(1)(C) (1998) (enacted). *See* discussion *infra* Part VI.C.3.

188 UETA Mar. 1999 Draft, *supra* note 69. Note: the other drafts which have been made public, referred to hereinafter by their labeled dates, are:

- National Conference of Commissioners on Uniform State Laws, UNIFORM ELECTRONIC TRANSACTIONS ACT (Jan. 29, 1999 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta199.htm> [hereinafter UETA Jan. 1999 Draft].
- NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, UNIFORM ELECTRONIC TRANSACTIONS ACT (Sept. 18, 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta1098.htm> [hereinafter UETA Sept. 1998 Draft].
- National Conference of Commissioners on Uniform State Laws, UNIFORM ELECTRONIC TRANSACTIONS ACT (July 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/98am.htm> [hereinafter UETA July 1998 Draft].
- National Conference of Commissioners on Uniform State Laws, UNIFORM ELECTRONIC TRANSACTIONS ACT (March 23, 1998 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta398.htm> [hereinafter UETA Mar. 1998 Draft].
- National Conference of Commissioners on Uniform State Laws, UNIFORM ELECTRONIC TRANSACTIONS ACT (Nov. 25, 1997 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta1197.htm> [hereinafter UETA Nov. 1997 Draft].
- National Conference of Commissioners on Uniform State Laws, UNIFORM ELECTRONIC TRANSACTIONS ACT (Aug. 15, 1997 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/ect897.htm>.
- UNIF. ELEC. COMMUNICATIONS IN CONTRACTUAL TRANSACTIONS ACT (April 10, 1997 Draft), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/ecomm.htm> [hereinafter UETA Apr. 1997 Draft].

189 *See* UETA Mar. 1999 Draft, *supra* note 69, §§ 102 (8, 15), 104, 106-109, 112.

190 *See id.* § 102 "Reporter's Note" ¶ 16; § 102(15).

191 *See* UETA July 1998 Draft, *supra* note 188, Prefatory Note, ¶ 3.

192 *See* Memorandum from Ben Beard, Reporter to the Uniform Electronic Transactions Act Drafting Committee and Observers (Jan. 29, 1999), *available at* <http://www.law.upenn.edu/library/ulc/uecicta/eta199m.htm> [hereinafter UETA Jan. 1999 Draft Reporter's Memorandum]; UETA Nov. 1997 Draft Reporter's Memorandum, *supra* note 69.

The UETA's operative provisions relating to digital signatures draw heavily[193] on the Illinois Act, the Massachusetts draft, a draft prepared by the Oklahoma Bankers Association,[194] and the UNCITRAL Model Law on Electronic Commerce. Thus, the UETA can be seen as a rejection of the Utah and California approaches (although some language drawn from the Illinois Act can be traced back, with revision, to those two sources).

The most controversial issue cited by the reporter to the NCCUSL drafting committee is the scope of the UETA.[195] Some proposed that it should, like other uniform laws, apply only to contractual documents.[196] On the other extreme, others proposed that it follow the Massachusetts and Illinois models and encompass "all writings and signatures."[197] The November 1997 draft proposed a compromise based on the UNCITRAL Model Law, covering not only commercial transactions, but also "electronic records and electronic signatures generated, stored, processed, communicated, or used for any purpose in any commercial . . . transaction."[198] In other words, it would have covered signatures and documents that are important for commercial reasons, but that do not themselves form commercial contracts.

In 1998, however, the drafting committee changed course again on the scope of the act, removing language that restricted the act to commercial or governmental transactions and related records.[199] Instead, the act applies to "electronic records and electronic signatures that relate to any transaction," although it also carves out a list of specific exceptions to which the act does not apply.[200] Substantively, the UETA would not apply to the creation or execution of wills or testamentary trusts.[201] Also excluded is

---

193 *See* UETA Apr. 1997 Draft Reporter's Memorandum, *supra* note 160.

194 *See* TECHNOLOGY COMMITTEE, OKLAHOMA BANKERS ASSOCIATION, DIGITAL WRITING AND SIGNATURE STATUTE (1996) (Second Discussion Draft), *available at* <http://www.abanet.org/buslaw/cyber/digsig.html>.

195 *See* UETA Jan. 1999 Draft Reporter's Memorandum, at 2; UETA Nov. 1997 Draft Reporter's Memorandum, *supra* note 69, at 2; UETA Aug. 1997 Draft Reporter's Memorandum, *supra* note 43, at 3; UETA Apr. 1997 Draft Reporter's Memorandum, *supra* note 160.

196 *See* UETA Nov. 1997 Draft Reporter's Memorandum, *supra* note 69, at 2; UETA Aug. 1997 Draft Reporter's Memorandum, *supra* note 43, at 3.

197 UETA Aug. 1997 Draft Reporter's Memorandum, *supra* note 43, at 3. Note, however, that the Massachusetts and Illinois drafts each include a so-called "repugnancy" clause, so the term "all writings and signatures" is misleading in any case. *See supra* notes 153, 164 and accompanying text. For a discussion of the UETA's history of addition and deletion of similar language see generally *infra*.

198 UETA Nov. 1997 Draft, *supra* note 188, § 103; UETA Aug. 1997 Draft Reporter's Memorandum, *supra* note 43, at 3.

199 *See* UETA Mar. 1999 Draft, *supra* note 69, § 103.

200 *See id.*

201 *See id.* § 103(b)(1).

most of the U.C.C., either because the articles themselves allow for the use of electronic signatures, or because state law has little impact in the specific area.[202] Lastly, the UETA allows state legislatures to identify other statutes for exclusion on a state by state basis.[203] Early drafts also contained "repugnancy" language similar to that in the Massachusetts draft and the Illinois Act (although among the UETA's then-limited scope of commercial or governmental transactions), providing that the UETA would not apply where repugnant to the manifest intent of the lawmaking body.[204] This language was deleted in early 1998, when the drafters decided a specific list of exemptions was needed.[205]

In its initial draft, the UETA, like the Illinois Act, had a two-tiered approach to the validity of electronic signatures.[206] Under this approach, a document would be "signed" if it "include[d] any methodology executed or adopted by a person with a present intention to authenticate a record."[207] The document would gain the benefit of some evidentiary presumptions (although like the Illinois Act, these were not as extensive as in the Utah law) if it were a "secure electronic signature" signed in accordance with a "security procedure."[208] The current draft, however, rejects the Illinois approach and streamlines this distinction.[209] Instead, a party must still prove the attribution of an electronic signature or record to a person (likely by showing the effectiveness of any security pro-

---

202 *See id.* § 103(b)(2)-(4) (excluding current or proposed articles 2, 2A, 2B, 3, 4, 4A, 5, 7, 8, 9, except for certain ministerial sections of articles 3, 4, and 4A).

203 *See id.* § 103(b)(5).

204 *See* UETA Nov. 1997 Draft, *supra* note188, § 104(a).

205 *See* UETA Mar. 1998 Draft, *supra* note 188, § 104 and Reporter's Note, ¶ 2. A more limited similar provision was re-introduced into the list of specific exclusions in the January 1999 Draft. *See* UETA Jan. 1999 Draft, *supra* note 188, § 103(c) and Reporter's Note to this Draft, ¶ 3. The drafters, however, felt that even this version introduced too much uncertainty, and deleted it in the March 1999 Draft. *See* UETA Mar. 1999 Draft, *supra* note 69, § 103(c).

206 *See* UETA Apr. 1997 Draft, *supra* note 188.

207 *See id.* § 102, ¶ 25.

208 *See id.* § 302.

209 *See* UETA Mar. 1999 Draft, *supra* note 69, § 108. In the July 1998 draft, the UETA drafters removed any separate definition of a "secure electronic signature," and evidentiary presumptions for signatures made under a security procedure. *See* UETA July 1998 Draft, *supra* note 188, Prefatory Note, at 4. Subsequently, an intermediate level of protection was proposed, in which signatures executed in accordance with a security procedure would be signed as a matter of law, but this was rejected in the January 1999 Draft. *Compare* UETA Sept. 1998 Draft, *supra* note 188, § 302(b)(2) Alternative 1 and Reporters Note, *with* UETA Jan. 1999 Draft, *supra* note 188, § 111 and Reporter's Note to this Draft. These enhanced protections were removed for fear that they would be applied to technologies that may be unacceptably weak, given that the UETA is technology-neutral. *See* UETA July 1998 Draft, *supra* note 188, Prefatory Note, at 4.

cedure that was used).[210] Notably absent, however, is the requirement of intent to sign the document.[211] Once attributed to a signer, the legal effect of the signature is determined from the circumstances of the signing or any effect given the signature by applicable law.[212]

The UETA drafters also recently added a section that would allow some electronic signatures to be equated with notarizations:

> SECTION 110. NOTARIZATION AND ACKNOWLEDGMENT. If a law requires that a signature be notarized or acknowledged, or provides consequences in the absence of a notarization or acknowledgment, the law is satisfied with respect to an electronic signature if a security procedure was applied which establishes the identity of the person signing the electronic record [and that the electronic record has not been altered since it was electronically signed].[213]

As discussed above,[214] while digital signatures are hard to forge, their guarantees are limited by their reliance on verification procedures undertaken long before the signing. Some of the security procedures referred to in section 110 could provide attribution and non-repudiation on par with a notarization.[215] However, the section should be clarified. To satisfy the purposes of a notarization, the procedure must establish the identity of the person signing the electronic record *at the time of the signing*. In addition, the UETA no longer provides any minimum floor for the sufficiency of a security procedure.[216] Furthermore, where the enacting state's laws require a sworn affirmation in order to have a legal acknowledgment or notarization, drafters should consider specifically requiring the electronic signature of witnesses authorized to administer oaths.[217] The present text seems to imply that such re-

---

210 *See* UETA Mar. 1999 Draft, *supra* note 69, § 108; § 108 Note to This Draft. The UETA definition of a "security procedure" is generic and technology-neutral:

> [A] procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the informational content of an electronic record.

UETA Mar. 1999 Draft, *supra* note 69, § 102, ¶ 15.

211 *See infra* notes 236-246 and accompanying text.

212 *See* UETA Mar. 1999 Draft, *supra* note 69, § 108(b).

213 *Id.* § 110.

214 *See supra* text accompanying notes 63-64.

215 *See* UETA Mar. 1999 Draft, *supra* note 69, § 110.

216 The January 1999 Draft deleted the former section 109, which considered the differences in treatment of a reasonable security procedure and one that would not be reasonable. *See* UETA Sept. 1998 Draft, *supra* note 188, § 109; UETA Jan. 1999 Draft, *supra* note 188, § 110 Reporter's Note.

217 By witnesses, I mean live witnesses present at the completion of the signing's security procedures. While it may be impractical to get the parties into a room, such a requirement does not undermine the reason for electronic communication in the first place, because

quirements are not necessary where electronic signatures are concerned, which would make virtually any cryptographic signature equivalent to a notarization.[218] Finally, the bracketed language concerning the ongoing integrity of the notarized message should be retained. Conventional notarizations do indeed serve to preserve document integrity by using embossed seals or stamps that are difficult to copy onto an altered version in an undetectable way.[219]

The UETA also delves deeply into the treatment of contracts formed where one or more of the parties is represented by an electronic agent, a computer program that binds the party (e.g., committing a vendor to shipping a product ordered on-line), although no human review of the agreement has occurred.[220] The UETA provides that a contract can be formed between a person and an electronic agent if the person takes actions she is free not to take, which she has reason to know will result in the agent completing the transaction.[221] The UETA January 1999 Draft deleted sections on "Manifesting Assent" and "Opportunity to Review" relating to "shrink-wrap" or "click-wrap" transactions.[222] Agreements where one party agrees to the terms of a contract merely by unwrapping product packaging or clicking on buttons or links on-screen, have been controversial in software licensing or electronic commerce. However, the UETA drafters deleted the provisions because they felt them to be unnecessary, not because they meant to dissuade such transactions.[223] Given the drafters' intention to allow such contracts, including the provisions would offer desirable certainty over the current reliance on a *Restatement* position, which is not necessarily the law in all states.[224]

---

notaries and witnesses are commodities reasonably available to any party undertaking a transaction requiring a notarization. It is even possible that such witnessing might permissibly be conducted by video-conference, with the (cyber-)notary affixing his signature remotely.

218 *See* UETA Mar. 1999 Draft, *supra* note 69, § 110.

219 *See id. But see id.* § 110 Notes to This Draft and Reporter's Note. UETA Reporter D. Benjamin Beard suggests that:

> The language [on document integrity] does go beyond what is generally the purpose of notarization, but was favored by some members of the Committee. . . . The purpose of a notary is generally one of identification, and so long as a security procedure establishes identity by the normal preponderance of the evidence standard, that should be sufficient.

Id. On the contrary, the use of an embossed seal, per se, gives no guarantee of the signer's identity. Therefore, its only purpose is to suggest that the document *is the same one that the notary embossed* (upon verifying the signer's identity).

220 *See id.* §§ 102(2), 102(6), 109(b), 113(b), 114.

221 *See id.* § 113(b)(2).

222 *See* UETA Jan. 1999 Draft, *supra* note 188, Reporter's Note to deleted §§ 107-108.

223 *See id.; see also* UETA Jan. 1999 Draft Reporter's Memorandum, *supra* note 192, at 3.

224 *See* UETA Jan. 1999 Draft, *supra* note 188, Reporter's Note to deleted §§ 107-108.

The UETA also addresses the legal viability of electronic records and authentication in creating electronic documents of title or other "transferable records."[225] The provision only applies to promissory notes, and not to chattel paper or documents of title.[226] This section is nonetheless notable because it suggests that electronic documents might technically suffice in real estate transactions, or other areas where electronic documents were thought to be inappropriate because one could not ascertain which digital "copy" was the authoritative one. In addition to traditional uses for transferable instruments, such instruments could also be invaluable in the area of electronic rights management involving serial copy protection schemes.[227]

The UETA is a promising proposal on many levels. Substantively, it strikes an appropriate balance between the flexibility of generic technology-neutrality and the specificity needed to keep from granting protection inappropriately. The UETA's lack of evidentiary presumptions for secured signatures is appropriate to its generic definition of a security procedure, as compared to the IECSA's and the Utah Act's reliance on the security provided by cryptographic digital signatures. As discussed below, in contrast with the proposed Uniform Computer Information Transactions Act, formerly U.C.C. Article 2B, the UETA might do well to reinstate the provision stating that securely signed records are signed "as a matter of law."[228] Likewise, the UETA's attention to its interrelation with the U.C.C. and other laws should help avoid unintended train wrecks on the track to a settled legal environment for electronic commerce.

Substance aside, a uniform statute is the most elegant device for addressing the validity of electronic signatures. First, national and multinational corporations already bemoan the proliferation

---

225 *See* UETA Mar. 1999 Draft, *supra* note 69, § 116.

226 *See id.* §116 Notes to this Draft. Chattel paper is excluded because the revised U.C.C. Article 9 already addresses electronic chattel paper. *See id.* § 102 Notes to This Draft ¶ 19. Documents of title are excluded merely because of lack of demand for their inclusion and because of the limited state presence in this area of law. *See id.*

227 For example, digital audio tape ("DAT") units are required by law to include a Serial Copy Management System ("SCMS"), allowing users to make copies from an "original" but not to make second generation copies. *See* Audio Home Recording Act of 1992, Pub. L. No. 102-562 (codified at 17 U.S.C. §§ 1001-1010). The SCMS is mandated in 17 U.S.C. § 1002. DVD units also include SCMS by agreement between manufacturers. These systems are becoming vulnerable, however, as the copy protection is imbedded in the playback hardware, but the content is becoming increasingly media-independent. An electronic transferable record might, for example, be used to embed *in the content data* indication of (license to) the right to make first generation copies, but prevent reproduction *from* copies.

228 *See* UETA Jan. 1999 Draft, *supra* note 188, § 111 (deleted Alternative 1, ¶ (b)(2)).

of discordant digital signature laws, each of which have indefinite jurisdiction over the global information infrastructure. Moreover, federal legislation may not be desirable because such sweeping action might stifle the evolving technologies, as will be discussed below.[229] Finally, a digital signature statute will have to harmonize with state law of contract and signature validity, much of which is shaped by the U.C.C. Existence of these competing concerns should be seen as a strong indicator that a uniform state law solution is preferred.

4. Uniform Commercial Code Revised Article 2 and Uniform Computer Information Transactions Act Provisions on Digital Signatures

The proposed Uniform Computer Information Transactions Act ("UCITA"), which was formerly to be Article 2B of the U.C.C., covering licenses, has also developed substantial provisions on electronic signatures.[230] Before the final text of the UCITA is approved, its drafters (which include the chair of the drafting committee for the UETA) intend to harmonize its provisions with the UETA.[231] Proposed revisions to Article 2 also include language tracking the UCITA.[232] Additional revision of the Article 2 language is on hold pending resolution of the issues by UCITA and UETA drafters.[233] Comments in the current Article 2 revisions suggest that the most satisfactory solution from a structural point of view would be not to include provisions on electronic signatures, but to allow them to be covered by the UETA or general revisions to Article 1.[234] However, this approach may not be possible unless one of these alternatives is enacted before the Article 2 revisions.[235]

Although consistency is the rule (and the goal) between the two drafts, the UCITA and the UETA will not contain identical lan-

---

229 *See infra* Part VI.C.

230 *See* U.C.C. § 2B-113 to -120 and definitions, § 2B-102 (Draft, Feb. 1, 1999), *available at* <http://www.law.upenn.edu/library/ulc/ucc2b/2b299.htm>. The NCCUSL and ALI have announced that what was to be the new Article 2B of the U.C.C. will instead be reported, by NCCUSL alone, as the Uniform Computer Information Transactions Act. As of this writing, however, no additional draft has been released under the UCITA name. *See NCCUSL to Promulgate Freestanding Uniform Computer Information Transactions Act ALI and NCCUSL Announce that Legal Rules for Computer Information Will Not Be Part of UCC* (Apr. 7, 1999), <http://www.nccusl.org/pressrel/2brel.html> (press release). Therefore, hereinafter citations to the UCITA will be to the still-operative Article 2B drafts.

231 *See* U.C.C. art. 2B prefatory notes, § 2B-113 note on status of part B.

232 *See* U.C.C. § 2-110 through 2-117 (Draft Revisions, May 1, 1998).

233 *See* U.C.C. art. 2 Comments to Part B (Draft Revisions, May 1, 1998), *available at* <http://www.law.upenn.edu/library/ulc/ucc2/ucc2598.htm>.

234 *See* U.C.C. art. 2 Comments to Part B (following § 1-218) (Draft Revisions, Feb. 1, 1999), *available at* <http://www.law.upenn.edu/library/ulc/ucc2/ucc2299.htm>.

235 *See id.*

guage, in part because the UETA has a much broader scope. Where the UCITA is limited to commercial licensing, the UETA applies to many non-commercial signatures and records. For example, the UCITA defines "authenticate" by the intention to perform any of several purposes an authentication may serve within the scope of that act, such as identifying the person, accepting a term or record, or confirming its content.[236] The UETA uses the much broader term "electronic signature," which merely requires that the signature is executed or adopted with the intent to associate the person with the record.[237] As discussed above, cases involving other developing technologies focus on the signer's intent to authenticate the document as with a normal signature, and those cases reached a rational result if they weighed the factor appropriately.[238] As such, the UCITA approach, by explicitly retaining the requirement of intent, is closer to the common law conventional wisdom concerning the essential properties of a signature than is the UETA.[239]

Most prominent among the substantive differences between the UCITA and the UETA is that the UCITA still includes evidentiary presumptions for signatures that use reasonable attribution or security procedures.[240] Where the UETA has deleted its provisions on the effect of a security procedure, the UCITA may instead de-

---

236 "Authenticate" means to sign, or otherwise to execute or adopt a symbol or sound, or to use encryption or another process with respect to a record, with intent of the authenticating person to:

> (A) identify that person;
>
> (B) adopt or accept the terms or a particular term of a record that includes or is logically associated with, or linked to, the authentication, or to which a record containing the authentication refers; or
>
> (C) confirm the content of the information in a record that includes or is logically associated with, or linked to, the authentication, or to which a record containing the authentication refers.

U.C.C. § 2B-102(4) (Draft Revisions, Feb. 1, 1999).

237 (8) "Electronic signature" means an electronic identifying sound, symbol or process attached to or logically connected with an electronic record and executed or adopted by a person with the intent to associate the person with the electronic record.

UETA Mar. 1999 Draft, *supra* note 69, § 102(8).

238 *See supra* Parts IV.B-C. Admittedly, this requirement has not been consistently applied. However, to the extent legislation is needed, it is to solidify this common law requirement, not to overturn it.

239 If the UCITA suggested that a signature served *all* the purposes mentioned in section 2B-102(4), it would clearly be too restrictive for the diverse applications of the UETA. Since a signature or authentication need serve only one of the purposes mentioned therein, however, there seems no need to define the term so minimally as does the UETA. *Compare* U.C.C. § 2B-102(4) (Draft Revisions, Feb. 1, 1999), *with* UETA Jan. 1999 Draft, *supra* note 188, § 102(19-20).

240 *See* U.C.C. §§ 2B-114 to -17, 2B-119. The UCITA indicates that the reasonableness of a security procedure can be established by statute, regulation, or in accordance with the purposes of the procedure and the parties' agreement. *See* U.C.C. § 2B-114.

lete the penalties for mandating unreasonable procedures.[241]

Giving effect to secure signatures is the inverse of defining the possible purposes of a signature. Where a mark is intended to have the effect of a signature (whatever that may be under the circumstances), defining it as equivalent to a signature or disallowing it to be thrown out because it is electronic, gives it validity. Where a symbol or process is unmistakably meant somehow to be equivalent to a signature, as is the case with complex procedures for secure signing, it is logical to assume something about the signer's intent in making the signature. The problem is that presuming specific facts about the signing is overreaching, for a signing may be intended for any of several reasons.

The UCITA makes such a mistake in providing presumptions that a record signed using a security procedure: (1) was signed by the purported signer;[242] (2) has not been altered since signing;[243] and (3) that the signer *intended* the signature to identify herself, to adopt the record, *and* to confirm its content.[244] The UETA makes the mistake of deciding that *nothing* can be assumed about the signing. In actuality, it is safe to assume that at least one of the many purposes of a signature was intended.

Such an assumption could be articulated by providing that a signature made with a reasonable security procedure is signed as a matter of law. Such a provision was deleted in the January, 1999, UETA Draft, but is still included in the UCITA.[245] The intent of the signature would be determined from the specific context, including relevant statutes, regulations or agreements between the parties.[246] Parties could still dispute what significance the signer intended by signing the record, but they would be foreclosed from arguing that no significance was meant by the signature. As mentioned above, familiarity with traditional signatures may operate

---

241 *See* U.C.C. § 2B-115 ("Effect of Requiring Commercially Unreasonable Attribution Procedure. Proposed for Deletion"); UETA Jan. 1999 Draft, *supra* note 188, former § 109 ("Determination of Reasonable Security Procedure" – Deleted); § 109 (former section 202 – deleted language whereby a record was attributable to a person if another person relied on a reasonable security procedure which so indicated); § 111 (deleted language providing that a signature verified in conformity with a commercially reasonable security procedure was signed as a matter of law); UETA Mar. 1999 Draft, *supra* note 69, former § 107 ("Effect of Security Procedure" – Deleted).

242 *See* U.C.C. § 2B-116(b).

243 *See id.* § 2B-117.

244 *See id.* § 2B-119(c). "As with common law signatures, an authentication can be used with several different intended effects . . . . In the absence of contrary indications present in the circumstances, the presumed intent encompasses all such effects." U.C.C. §2B-119 Reporter's Notes, ¶ 4.

245 *See* U.C.C. §2B-119(b); UETA Jan. 1999 Draft, *supra* note 188, § 111 (deleted Alternative 1, paragraph (b)(2)).

246 *See* UETA Sept. 1998 Draft, *supra* note 188, § 302 Reporter's Note.

like a presumption in their favor, putting electronic signatures at a disadvantage. Providing that a secure electronic signature is signed as a matter of law seems an effective way of eliminating any such discrimination without making unwarranted assumptions.

5. United Nations Commission on International Trade Law Draft Uniform Rules on Electronic Signatures

Since the approval of the Model Law on Electronic Commerce, UNCITRAL has been drafting a more specific set of Uniform Rules on Electronic Signatures, possibly to be adopted as an amendment to the Model Law.[247] Substantively, the Draft Electronic Signature Rules are like a cross between the Illinois and Utah Acts. The rules contain a two-tiered system for the recognition of electronic signatures generically, and "enhanced"signatures using security procedures,[248] but also contain detailed provisions for the regulation of certificate authorities.[249] The rules build upon the UNCITRAL Model Law. Therefore, they do not alter the basic provisions of that instrument, providing that records shall not be denied effect because they are in electronic form,[250] and that security procedures should be as reliable as is appropriate for their particular use.[251]

The UNCITRAL Electronic Signature Rules' provisions on signature validity are extremely similar to those of the Illinois Act.[252]

---

247 *See Draft Uniform Rules on Electronic Signatures*, U.N. Commission on International Trade Law, Working Group on Electronic Commerce, 34th Sess., U.N. Doc. A/CN.9/WG.IV/WP.79 (1998), *available at* <http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-79.htm> [hereinafter UNCITRAL Electronic Signature Rules Nov. 1998 Draft]. Note: the November 23, 1998, draft is not a complete text; the meeting from which draft document WP.79 resulted only discussed articles 1-15. *See Provisional Agenda*, U.N. Commission on International Trade Law, Working Group on Electronic Commerce, 34th Sess., U.N. Doc. A/CN.9/WG.IV/WP.78 ¶ 11 (1998), *available at* <http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-78.htm>. Therefore, for references to articles 16-19, see *Draft Uniform Rules on Electronic Signatures*, U.N. Commission on International Trade Law, Working Group on Electronic Commerce, 33rd Sess., U.N. Doc. A/CN.9/WG.IV/WP.76 (1998), *available at* <http://www.un.or.at/uncitral/english/sessions/wg_ec/wp-76.htm> [hereinafter UNCITRAL Electronic Signature Rules May 1998 Draft].

248 *Compare* UNCITRAL Electronic Signature Rules Nov. 1998 Draft, *supra* note 247, art. 2 ¶ 1, *and* arts. 3-6, *with* 5 ILL. COMP. STAT. 175/5-120, 10-120 (West 1998).

249 *Compare* UNCITRAL Electronic Signature Rules Nov. 1998 Draft, *supra* note 247, art. 12, *and* Chapter III, in general, *with* UTAH CODE ANN. § 46-3-309 (West 1998), *and* Part 3 in general.

250 *See* UNCITRAL Model Law, *supra* note 180, arts. 5-6.

251 *See id.* art. 7. The UNCITRAL Electronic Signature Rules do clarify, in commentary, that the appropriateness of a security procedure "would typically require the intervention of a judge, arbitrator, or other trier of fact" in every electronic signature case. *See* UNCITRAL Electronic Signature Rules May 1998 Draft, *supra* note 247, Remarks ¶ 17 (Remarks to art. 1). The benefit of a secure or enhanced electronic signature is that this appropriateness "would enjoy advance recognition." *Id.*

252 *Compare* UNCITRAL Electronic Signature Rules Nov. 1998 Draft, *supra* note 247, art. 2, ¶ 1, *and* arts. 3-6, *with* 5 ILL. COMP. STAT. 175/5-120, 175/10-120.

In both cases, informal electronic signatures may meet a basic threshold for validity.[253] This is unlike the Utah Act, which specifies no protection for such signings. In the UNCITRAL rules, an enhanced or secure electronic signature gains the rebuttable presumptions that: (1) the document was signed;[254] (2) the signature is that of the purported signer;[255] (3) the document's integrity is intact;[256] and (4) the purported signer is still liable for unauthorized signatures if he failed to take reasonable care to avoid such unauthorized use.[257] The provisions determining the validity of signatures are quite flexible, as they may generally be varied by agreement. Rather than a ceiling, they act as a minimum "floor" for signature validity where the parties do not have a prior contractual relationship, and as a "default" where they do.[258] While the Rules set forth circumstances in which a cryptographic digital signature may be considered an enhanced electronic signature,[259] the definition of an enhanced signature is not limited to digital signatures.[260] Therefore, other types of signatures may be proven to be enhanced signatures on an individual basis, or pre-determined to be an enhanced signature by agreement between the parties, or by domestic regulation.[261]

The UNCITRAL Electronic Signature Rules go well beyond the Illinois Act in specifying the responsibilities of certificate authorities. In this respect, the rules are quite similar to the Utah Act.[262] Interestingly, the UNCITRAL Electronic Signature Rules explicitly take the view that allowing the market to set standards for certificate authorities, as would happen in most states where authorities' responsibilities are not addressed, would be insufficient: "With respect to certification authorities, while the value of market-driven standards was recognized by the Commission, it was widely felt that the Working Group might appropriately envisage the es-

---

253 *See* UNCITRAL Electronic Signature Rules Nov. 1998 Draft, *supra* note 247, art. 2 ¶ 1 & arts. 3-6; 5 ILL. COMP. STAT. 175/5-120, 175/10-120.

254 *See* UNCITRAL Electronic Signature Rules Nov. 1998 Draft, *supra* note 247, art. 3. There are three variants to this article under consideration, and only one (Variant B) actually uses the term "presumption." All three, however, have the similar effect of shifting the burden of proof to the person seeking to discredit the signature.

255 *See id.* art. 4.

256 *See id.* art. 5.

257 *See id.* art. 7.

258 *See id.* General Remarks ¶ 14.

259 *See id.* art. 9.

260 *See id.* art. 1(b). In fact, the definition of an enhanced electronic signature is similar to the definition used in the California Act. *See* CAL. GOV'T CODE § 16.5 (West 1997).

261 *See* UNCITRAL Electronic Signature Rules Nov. 1998 Draft, *supra* note 247, art. 6.

262 *Compare* UNCITRAL Electronic Signature Rules Nov. 1998 Draft, art. 12, *and* Chapter III, in general, *with* UTAH CODE ANN. § 46-3-309, *and* Part 3, in general.

tablishment of a minimum set of standards to be met by certification authorities, particularly where cross-border certification was sought."[263]

With this in mind, under the UNCITRAL rules, a certified cryptographic signature is a secure or enhanced electronic signature if the signature was created during the operational period of the certificate.[264] Additionally, the issuing certificate authority must either: (1) be licensed by the enacting State;[265] (2) be "accredited by a responsible accreditation authority applying commercially appropriate and internationally recognized standards;"[266] (3) with respect to the certificate itself, it must have been issued according to internationally recognized standards;[267] or (4) there must be sufficient evidence which shows it accurately binds the public key to the signer's identity.[268] The UNCITRAL rules also address conflicts of law issues inherent in cross-border certification.[269] They allow for the issuance of a certificate from a foreign certificate authority, in an enacting state or to a signer in the enacting state.[270] The rules also allow the endorsement of foreign certificates by domestic authorities,[271] and the recognition of foreign certificates outright.[272]

The UNCITRAL rules contain several provisions limiting the liability of certificate authorities.[273] Unique to the rules is an article governing contractual liability between the certificate authority and its subscriber.[274] The rules essentially provide that such liability is controlled by the agreement itself, subject to applicable law.[275] However, the rules also allow certificate authorities to hold their subscribers liable for damage resulting from reliance on the certificate, unless it would be "grossly unfair."[276] This provision is

---

263 UNCITRAL Electronic Signature Rules Nov. 1998 Draft, *supra* note 247, Introduction ¶ 4.

264 *See id.* art. 9(1)(a).

265 *See id.* art. 9(1)(d)(i) (Variant A).

266 *Id.* art. 9(1)(d)(ii) (Variant A).

267 *See id.* art. 9(1)(d)(iii) (Variant A).

268 *See id.* art. 9(2).

269 *See* UNCITRAL Electronic Signature Rules May 1998 Draft, *supra* note 247, ch. IV.

270 *See id.* art. 17.

271 *See id.* art. 18. This article envisions, perhaps, international networks of affiliated certificate authorities, providing for the international acceptance of certificates through reciprocal contractual arrangements.

272 *See id.* art. 19.

273 *See* UNCITRAL Electronic Signature Rules Nov. 1998 Draft, *supra* note 247, art. 11-12.

274 *See id.* art 11.

275 *See id.* art. 11(1).

276 *See id.* art. 11(2). Synonymous alternatives to the term "grossly unfair," such as "inherently unfair and lead to an evident imbalance between the parties," and "unjustifiably give one party an excessive advantage" were offered. *See id.* These alternatives are drawn

questionable. It can be argued that the only reason for certificate authority liability in the first place is that the injured party cannot recover from the mischievous subscriber who gave the false information (a trickery the authority presumably failed to discover). If "Mallory" can be located and can satisfy a judgment, she should be liable. On the other hand, loss can also result from keys being compromised, the authority's negligence, or the failure of its verification apparatus. If, in every situation falling outside the subscriber's duty of care to safeguard the key, it is deemed grossly unfair to hold him liable, the provision may be acceptable. Otherwise, the result is that the subscriber's duty of care is made much higher than simply "reasonable," and the subscriber also becomes the insurer of the authority's operations. Both of these results would be unacceptable.

Regarding an authority's liability to relying third parties, the UNCITRAL rules take the position that no party's reliance is reasonable beyond the reliance limit of a certificate.[277] Admittedly, a relying party should not get away with entering a transaction in excess of the reliance limit because there turned out to be an error in the certificate (the possibility of an error being the very reason for reliance limits). However, the end result in the UNCITRAL law is identical to that in the Utah law, which was critiqued above. Where the authority complies with its obligations, it has *no* liability, and even where it is negligent, liability is capped at the reliance limit.[278] Again, a limit on liability, set by the authority itself, may be

---

from the UNIDROIT Principles on International Commercial Contract, art. 7.1.6. *See id.* at art. 11, remarks ¶ 51.

[277] *See id.* art. 12(2)(b). In total, the article limiting liability to relying parties provides:

> Article 12. Liability of the certification authority to parties relying on certificate
> (1) Subject to paragraph (2), where a certification authority issues a certificate, it is liable to any person who reasonably relies on that certificate for:
> (a) errors in or omissions from the certificate, unless the certification authority proves that it or its agents have taken all reasonable measures to avoid errors in or omissions from the certificate;
> (b) failure to register revocation of the certificate, unless the certification authority proves that it or its agents have taken all reasonable measures to register the revocation promptly upon receipt of notice of the revocation; and
> (c) the consequences of not following any procedure set forth in the certification practice statement published by the certification authority.
> (2) Reliance on a certificate is not reasonable to the extent that it is contrary to the information contained [or incorporated by reference] in the certificate [or in a revocation list] [or in the revocation information]. [Reliance is not reasonable, in particular, if [to the extent to which] it is:
> (a) for a purpose contrary to the purpose for which the certificate was issued;
> (b) in respect of a transaction, the value of which exceeds the value for which the certificate is valid; or . . . .

Id. art. 12 (alteration in original, denoting language under debate).

[278] *See id.*

an appropriate reward for a compliant authority, but a complete excuse from liability is inappropriately generous.

Finally, the UNCITRAL Electronic Signature Rules notably advance two concepts important to protecting privacy in a certificate authority infrastructure. First, the rules mandate disclosure by the authorities of "the policy or practices of the certification authority with respect to the use, storage and communication of personal information."[279] Second, the rules advance a distinction between certificates that require personal identification for the intent to sign, and certificates that verify other attributes of the holder (e.g., that she has $49.95 in the bank), but for which identity is superfluous.[280] Transactional information, such as a list of each site to which a certificate is presented, is easily aggregated by certificate authorities into sensitive personal profiles. Therefore, proactive consideration of the privacy impacts, by promoting the use of certificates which do not personally identify the holders, is welcome.

C. *Federal Encryption and Digital Signature Legislation*

As more and more states pass wildly different digital signature and certificate authority laws, federal legislators and lobbyists for large national and multinational corporations have made several proposals for federal legislation.[281] When considering federal legislation, however, two important concerns are present that are al-

---

[279] UNCITRAL Electronic Signature Rules May 1998 Draft, *supra* note 247, art. 16(2)(d).

[280] (e)"[Identity] certificate" means a data message or other record which is issued by a certification authority and which purports to confirm the identity [or other significant characteristic] of a person or entity who holds a particular key pair.

UNCITRAL Electronic Signature Rules Nov. 1998 Draft, *supra* note 247, art. 1(e).

> The definitions in subparagraphs (e) and (f) draw on the suggestion made at the 32nd session of the Working Group to distinguish the cases where digital signatures were used for the purposes of international trade transactions with the intent to sign (i.e., to identify the signer and link the signer with the information being signed) from other uses of digital signatures, for example, to establish the level of authority of a person ("authority certificates").

UNCITRAL Electronic Signature Rules May 1998 Draft, *supra* note 247, art. 1, Remarks ¶ 20.

[281] Most of the federal bills in this area have been proposed with fairly narrow interests in mind. For example, banks trying to be exempt from state digital certificate authority regulation benefit greatly from Senate Bill 1594. Computer companies possibly seeking to create a governmental market for their electronic authentication services were the only private sector witnesses at a mid-1998 hearing on the Government Paperwork Elimination Act. *See Hearing on the GPEA, supra* note 232. Similarly, law enforcement desires to encourage the use of key recovery encryption were the motivating factors behind the Secure Public Networks Act, S. 909, 105th Cong. (1998). For a discussion of the Government Paperwork Elimination Act see *infra* Parts VI.C.3. For a discussion of the Secure Public Networks Act see *infra* Parts VI.C.1. *But see infra* Part VI.C.4 (discussing Senate Bill 761, the Millennium Digital Commerce Act).

most wholly absent from consideration of state proposals: the preemptive effect of federal legislation, and the market-shaping force of the federal government's purchasing power.

Preemption of state digital signature laws would cut off the many developing state experiments aiming to develop the most viable solutions to this legal and regulatory riddle. Furthermore, such action risks preempting the valuable state consumer and regulatory protections found in many digital signature laws while leaving nothing in their place. Moreover, the signature requirements these laws address are intricately interwoven with states' common law of contract and with numerous state statutes. Even minimal enabling digital signature legislation on the federal level could preempt state digital signature laws, wreaking havoc on the functioning of state law and producing arbitrary differences between the status of electronic and traditional contracting.[282] That said, a proliferation of divergent state digital signatures eventually risks undermining the legal certainty needed to do business on-line.[283]

The federal government has in many cases sought to use its purchasing power to influence the market to further social policy ends.[284] As one of the largest purchasers of computer technology in the world, the federal government standards for purchasing products can have enormous market influence, whether politically motivated or not.[285] Electronic Signature technology is still in its infancy, and setting a standard for the acceptance of signatures by the government risks halting the market in its tracks. Companies would have less incentive to develop competing, incompatible products because they would be shut out of the federal market. Insofar as the legal environment shapes the functional requirements of products, a federal regulatory presence, such as federal licensure or registration of certificate authorities, would also shut out divergent business models. For these reasons, present reliance on state regulation and legal experimentation is preferable. Any

---

282 Such a result from federal legislation would be ironic, as a main purpose of digital signature statutes is to put electronic and traditional contracts into legal parity.

283 *See Hearing on the GPEA*, *supra* note 232 (testimony of Daniel Greenwood, Deputy General Counsel of the Information Technology Division, Commonwealth of Massachusetts, responding to questioning from Sen. Ron Wyden); *see also* Froomkin, *supra* note 31, § III.C.1. However, Froomkin argues such a preemptive action must not be taken until further evolution of the technology allows better comprehension of the law's practical application, and until a better sense of the functioning of different legal regimes has developed. *See id.* Part IV. Moreover, by that time, we should also have an indication whether the adoption of the UETA will alleviate the need for federal legislation.

284 *See, e.g.,* Adarand Constructors, Inc. v. Peña, 515 U.S. 200 (1995).

285 Indeed, in the encryption arena, the government tried to use its purchasing power, and restrictions on those educational and private entities that receive its funds, to coalesce key escrow encryption (the so-called "Clipper Chip") into a market standard.

federal legislation in this area should be narrowly crafted to avoid unnecessarily impeding the technology's development.[286] The only enacted legislation on the subject, the Government Paperwork Elimination Act,[287] already shows mixed results in this respect.

1. S. 909 - McCain/Kerrey Secure Public Networks Act

The 105th Congress' Senate Bill 909, the Secure Public Networks Act ("SPNA"),[288] focused on the contractual relationship between a certificate authority and a subscriber, an approach which was somewhat of a "cart before the horse." The SPNA would not have removed any of the potential obstacles to the acceptance of digital signatures, which is arguably a prerequisite to market demand for certificate authority services in the first place. Since the SPNA was primarily a bill to regulate encryption, it was not technology-neutral. In fact, it probably would have *imposed* obstacles to the acceptance of other forms of signatures, from informal electronic signatures to signature dynamics or biometric authentication. The SPNA contained liability limits even more drastic than either the ABA Guidelines or the already overzealous Utah Act.[289] Judging by the prevailing wisdom of state efforts, a critical problem with Senate Bill 909 was the fact that it would relieve certificate authorities from liability so completely.

The SPNA might also have had an effect on state drafting efforts through the doctrine of conflict preemption. A state statute is preempted where compliance with both federal and state regulations is a physical impossibility, or where state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.[290] Under Senate Bill 909, a state could

---

286 *See infra* Part VI.C.3,4 (discussing the Government Paperwork Elimination Act and the Millennium Digital Commerce Act).

287 *See* Omnibus Consolidated Appropriations, H.R. 4328, 105th Cong., Division C, Title XVII (1998) (enacted) (Government Paperwork Elimination Act).

288 *See* Secure Public Networks Act, S. 909, 105th Cong. (1998).

289 Compliance with the provisions of this Act and the regulations thereunder is a complete defense for certificate authorities and key recovery agents registered under this Act to any non-contractual civil action for damages based upon activities regulated by this Act.

Id. § 502.

290 *See* Gade v. National Solid Wastes Management Ass'n, 505 U.S. 88, 98 (1992) (citing Felder v. Casey, 487 U.S. 131, 138 (1988); Shaw v. Delta Air Lines, Inc., 463 U.S. 85, 95 (1983); Fidelity Fed. Sav. & Loan Ass'n v. De la Cuesta, 458 U.S. 141, 152-53 (1982); Jones v. Rath Packing Co., 430 U.S. 519, 525 (1977); Perez v. Campbell, 402 U.S. 637, 649 (1971); Florida Lime & Avocado Growers, Inc. v. Paul, 373 U.S. 132, 142-43 (1963); Rice v. Santa Fe Elevator Corp., 331 U.S. 218, 230 (1947); Hines v. Davidowitz, 312 U.S. 52, 67 (1941)). *See also* Pacific Gas & Elec. Co. v. State Energy Resources Comm'n, 461 U.S. 190, 203-04 (1983).

not have authorized a company issuing SPNA-compliant certificates to issue, as a separate product, non-SPNA-compliant certificates.[291] A state provision granting more limited immunity from liability than the SPNA's generous provisions would have been preempted as a direct obstacle to the federal registration plan. The state, therefore, would not have been able to apply the differential additional liability to authorities that were also federally registered. As such, the SPNA could have posed serious obstacles to the operation of state statutes regulating certificate authorities.

2. S. 1594 - Digital Signature and Electronic Authentication Law of 1998

Senate Bill 1594, the concise Digital Signature and Electronic Authentication Law ("SEAL")[292] specifically addressed the use of electronic and digital signatures by financial institutions. However, such regulation would have directly affected the certificate authority industry, as banks and other financial institutions are seen as the most likely candidates to become certificate authorities in a fully established public key infrastructure. SEAL provided that financial institutions could use electronic authentication when they agreed with another party, or as part of a transactional banking system.[293] Since many certificate authorities will be banks, SEAL would also have expressly limited states' ability to legislate with regard to digital signatures and certificate authorities:

> (2) STATE AUTHORITY-
> (A) IN GENERAL- No financial institution shall—
> (i) be regulated by, be required to register with, or be certified, licensed, or approved by; or
> (ii) be limited by or required to act or operate under standards, rules, or regulations promulgated by,
> a State government or agency or instrumentality thereof with regard to the use of electronic authentication, including acting as a digital certification authority or performing a similar role, pursuant to this Act.[294]

Therefore, SEAL would have reserved control of certificate author-

---

[291] [A] Certificate Authority. . . registered under this Act may issue to a person *a public key certificate* that certificates a public key that can be used for encryption only if the person [uses key recovery].
S. 909, 105th Cong. §§ 405, 407 (emphasis added). Note that key recovery was linked to the issuance of *any* public key certificate, not just SPNA-compliant ones.

[292] *See* Digital Signature and Electronic Authentication Law, S. 1594, 105th Cong. (1998).

[293] *See id.* § 6(a)(1).

[294] *Id.* § 6(b)(2).

ities to the federal government, without restoring the degree of regulation and consumer protection the statute would have displaced. Again, with methods of regulating digital signatures and authorities so untested, the advantages of uniformity are probably outweighed by the benefits of state experimentation with different regulatory paradigms. Moreover, SEAL represented an inadvisable avenue of regulation, because centralizing the electronic authentication and identity certification infrastructure would cause a dangerous consolidation of sensitive personal information. The information that such centralized authorities could collect would be rich enough to make the databases of the three major credit reporting agencies look like an office Rolodex by comparison.[295]

3. Government Paperwork Elimination Act

When originally introduced, the House and Senate versions of the Government Paperwork Elimination Act contained nearly identical text. However, their differing titles, the Senate's "Government Paperwork Elimination Act"[296] and the House's "Electronic Commerce Enhancement Act,"[297] betray the Act's schizophrenia. The Government Paperwork Elimination Act ("GPEA")[298] is caught between two competing objectives. On one hand, it aims to reduce government bureaucracy through electronic filing and document management.[299] On the other hand, it seeks to stimulate the growth of private-sector electronic commerce by giving consumers a convincing reason (namely convenient on-line interaction with government) to procure the tools necessary for its operation.[300]

As introduced, the GPEA mandated that nearly every federal

---

295 *See* Letter from the U.S. Public Interest Research Group and the Center for Democracy and Technology, to Senator Robert Bennett (May 1, 1998), *available at* <http://www.cdt.org/digsig/bennett.html>.

296 Government Paperwork Elimination Act, S. 2107, 105th Cong. (1998), *available at* <http://thomas.loc.gov/cgi-bin/query/z?c105:S.2107:> (as introduced); Omnibus Consolidated Appropriations, H.R. 4328, 105th Cong. Div. C, Tit. XVII (1998) (enacted) ("Government Paperwork Elimination Act").

297 Electronic Commerce Enhancement Act of 1997, H.R. 2991, 105th Cong., *available at* <http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2991:> (as introduced).

298 Government Paperwork Elimination Act, Pub. L. No. 105-277, Div. C, Tit. XVII, 112 Stat. 2681 (1998).

299 *See* S. REP. NO. 105-335, at 2 (1998); *Hearing on the GPEA*, *supra* note 232, (["The bill would] make unnecessary bureaucracy melt away.") (statement of Sen. Ron Wyden); ("The law still requires a pen and ink signature before [Members of Congress] can work with the agencies to resolve the constituents' problems . . . . Forms are unavailable, regulations require hard copies. We must remove these obstacles, and this legislation is an important part of that effort.") (statement of Rep. Anna G. Eshoo).

300 *See* S. REP. NO. 105-335, at 1 (citing "opportunity for enhanced electronic commerce"); *Hearing on the GPEA*, *supra* note 232 ("[T]he government can provide leadership in the development of consumer acceptance of on-line transactions . . . .") (statement of Scott Cooper, Manager for Technology Policy, Hewlett-Packard Company); *id.* (suggesting

form be made available on-line.[301] Forms must be available both for print-out and submission off-line through traditional channels, and for submission electronically, using an electronic signature where necessary.[302] Subsequent revisions by the Senate Commerce Committee clarified the timeline for implementation: (1) forms must be made available on-line within eighteen months;[303] (2) a timeline for implementation of the acceptance of electronic signatures must be prepared within eighteen months;[304] and (3) electronic submissions must be accepted within five years.[305] As finally enacted, however, the GPEA makes no separate mention of making forms available on-line.[306] This leads to the conclusion that no form need even be made available until the ultimate, five-year deadline.

Insofar as the GPEA seeks to improve government and private sector efficiency, this could be achieved on several levels. First and foremost, the government could reduce the cost of printing, storing, and shipping the millions of forms that citizens now have mailed to them or pick up at a local government office.[307] The GPEA could have more effectively addressed this aim than it ultimately did. This benefit occurs even if an Internet user prints the form and mails the hard copy. Electronic submission and, therefore, legislation on the effect of digital signatures, is superfluous to realizing a reduction in the cost of distributing printed forms. More significantly, since the provisions requiring the electronic availability of forms within eighteen months were deleted, even this benefit may not be realized until 2003.[308]

The government could also save money in the processing of returned forms if the data were to be submitted in electronic,

---

that a failure in the public sector to adopt digital signatures is impeding the progress of the technology and of e-commerce) (statement of Sen. Abraham).

301 *See* H.R. 2991 § 3; Government Paperwork Elimination Act, S. 2107, 105th Cong. (1998), *available at* <http://thomas.loc.gov/cgi-bin/query/z?c105:S.2107:> (as introduced).

302 *See* H.R. 2991 § 3; S. 2107 § 3.

303 *See* S. 2107 § 3(b) (as amended by the Senate Commerce Committee), *available at* <http://www.cdt.org/digsig/s2107.html>; *see also* S. REP. NO. 105-335, at 3.

304 *See* S. 2107 § 8(a)-(b).

305 *See id.* § 8(d).

306 The former section 3 of the Commerce Committee version, dealing with "Electronic Availability of Forms," was deleted in the final version. *Compare* Government Paperwork Elimination Act, Pub. L. No. 105-277, Div. C, Tit. XVII, § 1703, 112 Stat. 2681 (1998), *with* S. 2107 § 3 (as amended by the Senate Commerce Committee).

307 *See* S. REP. NO. 105-335, at 2 ("[T]he bill would save the government millions of dollars in costs associated with such things as copying, mailing, filing and storing forms."); *Hearing on the GPEA*, *supra* note 232 (statement of Scott Cooper).

308 *Compare* Government Paperwork Elimination Act § 1703, *with* S. 2107 § 3 (as amended by the Senate Commerce Committee).

machine-readable format.[309] Furthermore, industry could save money if often-submitted forms could be both submitted and archived electronically, instead of in paper form.[310] Insofar as many submissions of information may not require a signature, some of these advantages could also be achieved without addressing digital signatures. Further, one should ask what is really stopping agencies from taking these actions now? Representative Eshoo observes that existing law and regulations require hard copies, forbidding agencies from accepting electronic submissions in many cases.[311] If this is the stumbling block, then new law need only *allow*, not require, agencies to accept electronic submissions and signatures. Indeed, Andrew Pincus, General Counsel for the Department of Commerce, criticized the bill saying that, from the government's point of view, it should be enabling, not prescriptive.[312]

These shortcomings indicate that the GPEA could be nearly as effective at promoting government efficiency, while having less impact on the evolving electronic authentication industry. Therefore, the law is perhaps best viewed as an incentive for electronic commerce. Comments by representatives of some companies indicate that their goal in advancing the bill is, in part, to make the federal government a laboratory for the continuing development and evolution of electronic signature technology and implementation.[313] One way this is accomplished is by the Office of Management and Budget setting "technical standards,"[314] "guidelines,"[315] or "procedures"[316] for the government's acceptance of electronic signatures, within a year and a half after passage. Given the enormity of the project of implementing the GPEA, the Federal Government is the one entity that should not be a guinea pig. The federal government, just by virtue of which experiment it chooses to run, may create a de facto standard at a time when the technology is still uncertain.[317] The many state paradigms that are being

---

309 *See* S. 2107 § 3 (as amended by the Senate Commerce Committee).

310 *See id.*

311 *See Hearing on the GPEA*, *supra* note 232 (statement of Rep. Anna Eshoo).

312 *See id.* (statement of Andrew Pincus, General Counsel, U.S. Department of Commerce).

313 *See id.* ("We are very happy to volunteer the federal government as a guinea pig . . . . We're not looking for perfection.") (testimony of Scott Cooper, Hewlett-Packard).

314 H.R. 2991 § 7(a).

315 Government Paperwork Elimination Act, S. 2107 § 5(c), 105th Cong. (1998), *available at* <http://thomas.loc.gov/cgi-bin/query/z?c105:S.2107:> (as introduced).

316 Government Paperwork Elimination Act, Pub. L. No. 105-277, Div. C, Tit. XVII, § 1703(a)-(b), 112 Stat. 2681 (1998).

317 *See Hearing on the GPEA*, *supra* note 232 ("[F]ederal legislation of this type must stop short of picking technology winners and losers before the market has finished evolving the

developed are preferable as experiments; unlike the federal government, if a state sets a standard, the market will not ossify as a result.

Aside from the questionable propriety of setting federal standards for electronic signature technology, and the final act's failure to require the near-term availability of forms on-line, other added provisions help provide for flexibility in implementation. For example, certain forms may be excluded if placing them on-line or accepting their submission electronically would not be "practicable."[318] The five year period before the acceptance of electronic signatures is mandated should also allow the market for signature technologies to mature before implementation.[319] Further, the bill also mandates technology-neutrality, where appropriate.[320] The final GPEA also includes laudable privacy protections, prohibiting the disclosure of personal information that certificate authorities might collect in the course of enabling electronic communication with the government.[321]

Perhaps the real motivation behind the GPEA is that individual computer companies clamor for the mandate, through legislation, of a governmental market for the hardware and software necessary for publishing and accepting electronic documents on a massive scale.[322] On the other hand, the depth of the federal government's role in setting the technologies to be used was actually scaled back markedly between the bill's introduction and its passage.[323] Perhaps this occurred because of other elements of the

---

best solutions.") (statement of Daniel Greenwood, Deputy General Counsel of the Information Technology Division, Commonwealth of Massachusetts).

318 *See* Government Paperwork Elimination Act § 1704.

319 *See id.* However, the fact that the procedures are set within eighteen months could, depending on the specificity of the procedures at that point, eliminate such flexibility.

320 *See id.* at § 1703(b)(1)(B).

321 *See id.* at § 1708.

> Except as provided by law, information collected in the provision of electronic signature services for communications with an executive agency, as provided by this title, shall only be used or disclosed by persons who obtain, collect, or maintain such information as a business or government practice, for the purpose of facilitating such communications, or with the prior affirmative consent of the person about whom the information pertains.

Id. Where the Utah Act and other models have been criticized herein for failing to advance consumer protections alongside the advancement of electronic technologies that tend to erode such protections, the GPEA is commendable for trying to ensure that citizens do not take a privacy "hit" by interacting with government on-line.

322 *See Hearing on the GPEA*, *supra* note 232 (stating that the bill is "vitally important," in that it will help jump-start electronic commerce) (statement of Kirk Le Compte, Vice President of PenOp, Inc.); *see also id.* (statement of Scott Cooper, Hewlett-Packard).

323 Again, the government was to set "technical standards" in the original House Bill 2991, but in the enacted version the government was merely to set "procedures." Among other changes, the explicit requirement of technology-neutrality was also added. *See* Government Paperwork Elimination Act § 1703(b)(1)(B).

electronic commerce industry growing nervous over having the federal government driving the technology. At any rate, this is a rare occasion where the law risks being ahead of the technology. Ironically, we might profit from the federal government's lagging a little further behind the cutting edge.

4. S. 761 – Millennium Digital Commerce Act

Introduced March 25, 1999, by one of the principal sponsors of the GPEA, the Millennium Digital Commerce Act ("MDCA")[324] is the 106th Congress' first attempt at digital signature legislation. It is also the first federal bill primarily concerned with the validity of electronic transactions in the private sector.[325] The drafters of MDCA are clearly aware of the possible preemptive effects of federal legislation and are attempting to minimize such preemption.[326] In fact, the most noteworthy aspect of MDCA is that it attempts to use federal law as an interim measure for providing certainty, *until and unless* states enact the UETA.[327]

The MDCA contains two principle operative sections.[328] The most significant section is section 6, "Interstate Contract Certainty," which sets out substantive defaults for the validity of electronic signatures, as well as for the MDCA's relation with state law.[329] Substantively, the bill provides (in language modeled on the Massachusetts draft and the UNCITRAL Model Law) that, "[a] contract relating to an interstate transaction shall not be denied legal effect solely because an electronic signature or electronic record was used in its formation."[330] The bill also gives the parties to a transaction the ability to choose acceptable methods for using electronic signatures, notwithstanding laws allowing or requiring specific methods.[331] After enunciating this basic substantive core, the bill attempts to make these provisions apply only in the absence of the UETA or another consistent statute:

---

324 *See* Millennium Digital Commerce Act, S. 761, 106th Cong. (1999), *available at* <http://thomas.loc.gov/cgi-bin/query/z?c106:S.761:>.

325 *Compare id.*, *with* Government Paperwork Elimination Act, Pub. L. No. 105-277, Div. C, Tit. XVII, 112 Stat. 2681 (1998) (intended as government efficiency legislation), *and* S. 1594, 105th Cong. (ostensibly limited to financial institutions), *and* S. 909, 105th Cong. (encryption legislation).

326 *See* S. 761 § 6(c); Abraham, *supra* note 161.

327 *See* S. 761 § 6(c).

328 *See id.* § 5 ("Principles Governing the Use of Electronic Signatures in International Transactions"), § 6 ("Interstate Contract Certainty").

329 *See id.* § 6.

330 *Id.* § 6(a). Note that like most digital signature laws and analogous common law, but unlike the UETA January, 1999, Draft, the MDCA retains the requirement of intent in the definition of a signature. *See* S. 761 § 4(7); *see also supra* Parts IV.B-C & VI.B.4.

331 *See* S. 761 § 6(b).

> (c) Not Preempt State Law.— Nothing in this section shall be construed to preempt the law of a State that enacts legislation governing electronic transactions that is consistent with subsections (a) and (b). A State that enacts, or has in effect, uniform electronic transactions legislation substantially as reported to State legislatures by the National Conference of Commissioners on Uniform State Law shall be deemed to have satisfied this criterion, provided such legislation as enacted is not inconsistent with subsections (a) and (b).[332]

The MDCA recognizes that the ultimate solution for digital signature legislation may be a uniform state law, rather than a federal law.[333] Assuming that this mechanism for reversion to a state law solution is applied by courts as intended,[334] it may represent the most helpful role for federal legislation to play in the evolution of digital signature law.

The other operative section of the MDCA concerns international applications of electronic signatures, providing principles for the federal government to observe in enabling international transactions.[335] These include adopting the UNCITRAL Model Law, allowing parties to set their own authentication technologies, and recognizing signatures from other countries.[336] It is unclear, however, whether the provision is meant to have any binding effect on domestic law or policy. Apparently, the section is primarily aimed at bolstering the U.S. negotiating position against other countries which attempt to grant preferential treatment to domestic signatures.[337]

Although there are some questions to be addressed within the bill,[338] the MDCA would be a valuable measure for providing short

---

332 *Id.* § 6(c).

333 *See id.*; *see also* Abraham, *supra* note 161.

334 An adequate analysis of preemption precedents involving statutes with language similar to the MDCA is beyond the scope of this Article.

335 *See* S. 761 § 5.

336 *See id.*

337 *See* Abraham, *supra* note 161.

338 Undoubtedly the MDCA is, as this Article is being published, at an early stage in the legislative process, and will be revised as it progresses. At this stage, however, drafters would do well to correct three shortcomings.

First, the MDCA specifies that the UETA is deemed consistent with it, "provided such legislation as enacted is not inconsistent with subsections (a) and (b)." S. 761 § 6(c). This language could be interpreted to mean that the UETA satisfies the MDCA so long as the UETA, as actually reported to the states, is consistent with the MDCA. More likely, the language may be intended to mean that enactment of the UETA satisfies the act so long as the individual state did not alter the UETA so as to make it inconsistent with the MDCA. Given that the drafters of the MDCA anticipate that the UETA will be reported by October, 1999, *see* Abraham, *supra* note 161, by the time the MDCA might approach passage, it will be known whether the reported UETA is satisfactory. Therefore, the language could be changed to, "provided any differences between such legislation as enacted and the legisla-

term certainty in electronic contracting. First, its operative provisions have been reduced to bare, essential, enabling language; to the extent the bill would preempt state law, the resulting conflicts would be minimal.[339] The bill does not set up a federal regulatory infrastructure, nor interfere with state regulation of certificate authorities. It is completely technology-neutral, and does not provide for technological standard-setting, even for the federal government's use of electronic signatures.[340] Most importantly, the bill appears to recognize that state law is the best forum for digital signature law, and is intended to function only as an interim measure, providing further incentive for states to adopt the UETA.[341] By the time the UETA reaches final status, the MDCA may be ready for passage, at which point the MDCA could be a successful way to bridge the gap until the UETA has been enacted by the states.

VII. Conclusion

Fundamentally, the case law bearing on the validity of digital signatures is still unformed. At least as to the basic validity of writings and signatures in electronic form, the case law may very well adapt acceptably. This has generally happened with the development of the fax, telegram, telex, and so on. As to more secure methods of signing, case law is non-existent, so there is little basis from which to draw a conclusion either way. This suggests that the interest propelling digital signature legislation is not the correction of deficiencies in judicial interpretation; such deficiencies have not been demonstrated. Rather, drafters should recognize that stimu-

---

tion reported to the States legislatures by the National Conference of Commissioners on Uniform State Law do not make the enacted legislation inconsistent with subsections (a) and (b)."

Second, the MDCA provides that state laws must allow "parties to an interstate transaction" to choose their methods of electronic authentication by agreement. *See* S. 761 § 6(b). While this is a valuable principle in general, this blanket provision would be unhelpful if it allowed parties to validate electronic records and signatures in situations specifically excluded from the UETA. Even worse, because state law is preempted unless it is consistent with this provision, even after a state enacts the UETA, such exemptions from the UETA would be preempted. While some of the most notable examples (such as wills) might not pose a problem because they may not be considered "interstate" or "transactions," federal drafters might, nonetheless, need to address the thorny issue of exclusions from the bill's coverage.

Finally, the purpose of the section on international transactions should be clarified. If it is meant strictly as a backdrop to negotiations with other nations, the section may be unnecessary, as it appears that the Clinton administration is already taking this position, without such laudatory advice from Congress. *See* Abraham, *supra* note 161 (mentioning already demonstrated support for this position by the Departments of Commerce and State). If it is meant to have domestic effect, that effect should be clarified.

339 *See* S. 761 §§ 6(a)-(b).

340 *See id.* §§ 2(3), 2(7), 5(2), 6(b).

341 *See id.* § 6(c).

lating electronic commerce is really the driving force behind preempting the normal accretion of judicial precedent. Once this recognition is made, perhaps policymakers will reevaluate whether subsidizing electronic commerce companies is so compelling a reason, and they will more narrowly tailor their proposals to the narrow obstacles that may exist for the recognition of electronic signatures.

While many states' laws on digital signatures are still in development, much study and consideration has already gone into various drafting efforts. More recent state laws and draft proposals show an increasingly mature examination and understanding of the issues attendant to digital signatures, as well as the needs of industry in the matter. In short, the state "experiments" which flourish in the absence of federal legislation are increasingly productive. Therefore, if one accepts the need to legislate, the present trajectory seems satisfactory. Moreover, a comprehensive examination of the emerging legal issues informs the drafting of the Uniform Electronic Transactions Act, arguably the most appropriate forum for further development. Hopefully, the UETA can integrate the lessons of the preceding state efforts, harmonize with existing state laws and developing international efforts, and restrict its actions to those necessary to bring existing law of attestation into the information age.

EXHIBITS

Exhibit 1: Example of a Public Key for Encryption and Signing

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Personal Privacy 6.0.2

mQGiBDOezdARBADAkydG7kqlXOkQA8j5r61bbg5UwvcAyXZSHJPW4lh4N4RUkOkX
ENRQPOaWc8jiKpU2tavy6ge61PGR85XiF1xgvHvh3l6nDsZiurlMG8yRMYXHa0zx
4xaWyghcsVVFV5e3wX46aHch1/ofePlkAZ7W4aYN/vyXD9KR2vKcRchI8wCg/x4x
ttbWvktC8fAcuyMVNRroC8UD/2IidquBiBtHqTGy9076i+mLqIeRj+ZbhsEYaPgc
TxJNnxotebh/dywrkv9DSN2wty7OnJ4k6gg40SnNaYHEQp/gfvUCablY1tlEx/c+
Kt/b4hBTgFc8xmstAYcM4sWTVWG39SRAH4XRYL9KuWhpt0bjxrQocMuQ3P0Db2ki
U8BrBACDVSzj4iXkxaADZ9Ul9oQdrJTmjpej/4/YzTT8ZMvLP38gHzqZOpy5+fk+
3z+cn1K7RADZw5URDPYXGlZ/+CEA8Bi1K6EP2RqLwv2A4L+ZdHd182pV5c2R4818
FBJQOeHAINFKY6+faU6fukzRtD6zpYSQWr5HtSr85cIld1EzOrQqQWRhbSBXaGl0
ZSBTY292aWxsZSA8YWRhbS5zY292aWxsZUBiYy5lZHU+iQBLBBARAgALBQIzns3Q
BAsDAQIACgkQCqenawCHJh0w+gCgwkBSq1jwzN0pA5xVdd1Kb8/uyeUAoLa3TgXR
FNnWsXr/JVauT6mUAO+ziQCVAwUQM7I7HO4VT9g16YzVAQFW+wP/aDLa9j5xrGya
6CGpCVYSDrb1JLv2mz7iOwQiGWQnxSScHV4+AM7hW7PFVD4Y3eQj+jx5+4Zhrubc
kxE7SezaZC4RTyY25DDLUM4IIRNz5sGVZa1cBRH7rvdNpsUbz8lRm4HMGAzmOwOX
fAaEn17lYAUnzcSgUcfJISCKy+owrR+JAJUDBRAz6McLNCtBZUNTKw0BAS11BACM
Ohlg+P6vDKTginBCCZ4GStvBImgFmQhiq+TWv7macStHx1xhyi8+HcCeHE/WM929
0Zd9huqQOOfVmA86xRT4GfO9u4nIVaLjmwtg4ot8C3V4j1S7arGhrBWWwyZvPM4L
auo4cUSJicMdZ+m44Ld4hG6E/qbJu3SOn47/1dSrY4kBFQMFEDQq9NL2pIahfBNw
0QEBwjoH/1M1ZHYFgrVrOKf0ty10lu8Hc5Uh0duirpgGg4qxIa3fpjSZG9CD0CRK
4eqpfIbCMM8N7NCb6R5Jywm8LBp/DrxvI8kBFlJ/rgoj3OG6i81CkC/H0YFdcbIx
gZ9XzqvgVjSmpCr+YkoxXTrj0nDePMOHInh7n9L/5Js2JLI2HulQZBwn+2a5sMym
M+oGnExsYKSeWg52W4CYZEaZTgNp1U6CkfExiU1sfN1DT7xZHVSHfPU4NJPcp755
JcYqVY1EQpCvXvIqEnP3mzS7vUSgbQBehL01n+NwTmb7NbHN6WcoN2j1zshklvxY
PISmI0hKMLRxJ1GmYHhY1x1ClcHiS9y0JUFkYW0gV2hpdGUgU2NvdmlsbGUgPGFk
dmlsbGVAY2R0Lm9yZz6JAEsEEBECAAsFAjOz3BgECwMBAgAKCRAKp6drAIcmHQX4
AKCtVSAR0jvyUnbGEcRzJIPff1nodwCgwcgsZBiNncngYs5ov8NUfxm9uc2JAJUD
BRAz6Mc2NCtBZUNTKw0BAX/gA/4kzCNew/4TYnkBp/aPC/XKTBzazaD1sqIyaB1p
HBI1kgCtw6I62Yqf/D1BxQgXEM2dqz/6BWUZrQRk6XxbbQ4Jp6vrmjaSzgouVUOM
fL2/8FKyYe/M7nJmv5hPXVOpiX5wOvdnhRbV+/J/xWkzStUVgxpvqDWpr3+tPyNn
LoQwB7kBDQQzns3qEAQA9RGZdFhe5nEV4X4Zl19nmSwhjNfZOFLCww7Jcq38Gpii
rVCCTL4AaPLRJb7I9m36qDqqHYkfv4gXPDeM1YsoPIxXQ9APjRTdo0x35+xo053W
rIoGjCjQzWlV4uf5t1ZRQG4FLu2yKjWJqCkqvk/iVNemqpPOqd2+kBd/tySLAwkA
AgIEAJ/zqA4bj22sBwJ9VFnx79yi0e6ZVGqqm8C+nxvjpwZyDKUTED8Ix9AdGpr4
MY0qLWxX601dr9Rbyf/v5UWIECTgIAFHJjbZl3ScpPEvJi0XgvuWsRak+NCSdbHP
lwRZ16E09oD1aou4S9om/827jJjZzr3lcN3YltdeUf1/zk1KiQA/AwUYM57N6gqn
p2sAhyYdEQJZxwCeKMKSevm4h3uwVNI+WGpXV9j8ifYAnA5Y49z84/WzNBRurm0U
teZK3r7f
=cAXu
-----END PGP PUBLIC KEY BLOCK-----
```

Exhibit 2: Example of a Cryptographically Signed Message

```
Date: Wed, 13 May 1998 17:42:31 -0400
To: adam.scoville@bc.edu
From: "Shabbir J. Safdar" <shabbir@mindshare.net>
Subject: Acceptance of Offer

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

May 13, 1998

Dear Mr. Scoville:

On behalf of MindShare Internet Campaigns, L.L.C., I hereby accept your
offer to license from us a 10 user copy of our specialized internet
lobbying software, MindWidget 2.0 for $14,500. This is subject to the terms
of the electronic license included with the downloadable software. The
disabled demo version you downloaded will become fully functional upon
entering the registration codes which are being sent to you in a separate
message. MindShare guarantees that use of the product will yield at least
10,000 pieces of constituent electronic mail SPAM sent to congressional
offices within the first month, or you may erase the program and have 80%
of the license price refunded to you.

Shabbir Safdar
for
MindShare Internet Campaigns, L.L.C.

Note that this is a message for test purposes only for a demonstration of
how to use encryption.  mindshare does not have a MindWidget product, and
if we did, we'd certainly not license it for less than six figures.


- ------------------------------------------------------------------------
Shabbir J. Safdar                                   shabbir@mindshare.net
mindshare Internet Campaigns, L.L.C.             http://www.mindshare.net/
PGP-encrypted email encouraged                      Phone: +1.202.887.7071
- ------------------------------------------------------------------------


-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.5.3

iQA/AwUBNVoT7FI7X4uZXBpJEQIfnQCggH2gUISJicmA2YqTft5YVuVyMo0AoLdX
t3TuoIp7nkKNGjoe2FqWcxtB
=Gp37
-----END PGP SIGNATURE-----
```

Exhibit 3: Cryptographically Signed and Encrypted Message

```
Date: Wed, 13 May 1998 14:07:00 -0400
To: adam.scoville@bc.edu
From: "Shabbir J. Safdar" <shabbir@mindshare.net>
Subject: Acceptance of Offer

-----BEGIN PGP MESSAGE-----
Version: PGP for Personal Privacy 5.5.3

qANQR1DBwE4DVep2Bpg7Aq8QBACWl28Bl8BWjYpCTMGSdmBfEGhuTJBtXKBtN/8e
zs4pWxtMCX0mYkFtkkTQCVxsvlrIY8E5h8sVoN5M2hPQXo5d8S+uqLRgFXZoq+rt
8tSY7NTPiW6/kLcHMtrXqpRPYeOBoTzuooOMQ+jcCoTnAxmHhfJ7W0NJyYMTT/Ee
+l0kZQQAsf/eb4P18UuC1XjAXuJC8b1TbVpVG3vKHW1chgeFpTJ4ri20WHqNZ/tj
FSPA+md7ND0uu6KLg5Lw01jFv2fna8BUejm1/sStAm7ywIQoa8/OGjKNH+mIGEnp
fEIgVe+63VSLp7wLqZdUx1pAJpduocHC2phjQ4qOagVMFp7I0UHJwggGZnLlCiGm
bd/Uh2mRF2hcaZ0X2bJTJNXgOwtM0jS2OBiAhnNHXDer6YNGbk1QrtA0tyXKk+IR
fo6eq9gNR1Asp66d4zLPJJD7jNc6fGaYgGbKze2QyqkN+zc0Afdq72l+obwcWa6f
1az8Ie/MQi/uJEwScK7dhDyz9obg1CEnA12q8y0BgyTZxqbWNgVLCySrNMf7SkpU
88kyP5HiV+muCR31IZ6wxc9l6IF5OOaVfPIO9aB2B05/Jp2V1dSvnqxvE48jqz2n
tCVQwbLw6HAqWO3079Bupo+hN3IeMY9DNrPmDPuJhSkoU7i0gKpuzywNaVxnHoAp
fvy8HC6tWiv5UlsUT5bsA+YEQbfwYqyguNptfXbNsq1GJwdjnXgVwBBedoFTwbwq
HKjN+ZCkhFm7oX6cSLbDmnUF/q5E9BmthEK5EaOo6nbiTtWZ/lj4NjtXhzDkPcZK
b8fAVusAElxhbxFdqzFKVCRH2UBUyDrVVM7cjF0F9NiW8Pys4o5c4+9kl9HJ2djm
Bt8MMPj5aIiitEtT0jVzWlEDF3uVJEipKVUsD0ZzpABQVL9houIwV6WWhyCG+2vB
3oahSwmHuYZt6WdtoR+arQ1fR6HyUKvjo+1SDKvXK6FUJ+KzkzvcXFjBX13JebgL
dxVoaXDEyb2DL6Dg9YN7VWuhGVjC1CC7d69xtArXQETckleVQ7XuwQCZhV2p5ECl
gd/kYrHz+GbIatcAkQSVn2EqfvKmmUCMdXBkRgNVMkU1cDa2aX+QKDS29u8bPF8T
nhmrUqrH0hGUqwtn5eAlz2t6kQ15cJ5XsIblFgoCvfqTP3EkcpCO0MYqNtzMBU4X
UYhlP4KsDeMDuvmNGArs2/1kQlBh66Tubbe6odsvr4Fc5dl5W+7oCdr4gEcusf0G
a/n6iSDC+2bfHDdxr2tz+Azt/c7/tTIGRhkqHipQfHWl
=VzP7
-----END PGP MESSAGE-----
```

Exhibit 4: Alteration of Signed Message Indicates New Signature

```
Date: Wed, 13 May 1998 18:35:31 -0400
To: adam.scoville@bc.edu
From: "Shabbir J. Safdar" <shabbir@mindshare.net>
Subject: Acceptance of Offer

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

May 13, 1998

Dear Mr. Scoville:

On behalf of MindShare Internet Campaigns, L.L.C., I hereby accept your
offer to license from us a 10 user copy of our specialized internet
lobbying software, MindWidget 2.0 for $4,500. This is subject to the terms
of the electronic license included with the downloadable software. The
disabled demo version you downloaded will become fully functional upon
entering the registration codes which are being sent to you in a separate
message. MindShare guarantees that use of the product will yield at least
10,000 pieces of constituent electronic mail SPAM sent to congressional
offices within the first month, or you may erase the program and have 80%
of the license price refunded to you.

Shabbir Safdar
for
MindShare Internet Campaigns, L.L.C.

Note that this is a message for test purposes only for a demonstration of
how to use encryption.  mindshare does not have a MindWidget product, and
if we did, we'd certainly not license it for less than six figures.


- ------------------------------------------------------------------------
Shabbir J. Safdar                                   shabbir@mindshare.net
mindshare Internet Campaigns, L.L.C.             http://www.mindshare.net/
PGP-encrypted email encouraged                     Phone: +1.202.887.7071
- ------------------------------------------------------------------------


-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.5.3

iQA/AwUBNVogRlI7X4uZXBpJEQJjbQCgo0/THATqgC3FJFosxO187nnr4vgAmwQj
jNVjZ6Fi13v5Fxi+ICIDwWS9
=T0Nh
-----END PGP SIGNATURE-----
```

Exhibit 5: The ease of forging electronic documents and signatures - a fictitious example

THE WHITE HOUSE

April 31, 1999.

Dear Mallory,

I want to thank you for your discretion over the past year. I know it's been hard for you to put off the constant calls from Mr. Starr and Mr. Drudge. Believe me though, that it's for the good of the country to avoid re-entering that nightmare. Things should quiet down again once the IC statute lapses.

But what I'm really writing about is to confirm my offer to you of a position in the White House Travel Office, starting at your earliest convenience, for a period of a year and a day, and renewable thereafter, at a salary of $36,300 per year.

Sincerely,