Electronic Commerce Legislation:

From Written on Paper and Signed in Ink

to Electronic Records and Online Authentication

By Daniel J. Greenwood and Ray A. Campbell*

The explosive growth of the Internet during the past twenty years[1] has created opportunities for electronic commerce and other online transactions that were unimaginable only a few years ago.[2] According to some estimates, by the turn of the century the value of electronic commerce transactions in the United States alone will reach tens of billions of dollars per year.[3] The growth of electronic commerce is affecting virtually every sector of the economy and has attracted the attention of policy makers at every level of government.[4] As a result of this attention, there is a growing realization that electronic commerce will only achieve its full potential if there is a modern legal infrastructure that supports the use of online technologies for business and government transactions.[5]

Despite the rapid acceptance of online technologies in general, and of the Internet in particular, there remains a widespread perception that using the Internet for important transactions is subject to significant security and legal risks. The security risks are a function of the open and decentralized nature of the Internet. Rather than being a single and centrally controlled network, the Internet is a network of networks in which messages are passed from computer to computer on the way to their destination.[6] This architecture creates the risk that a message can be intercepted, or even altered, on its way to the intended recipient. To address

these concerns, scores of firms are developing products to improve the safety of Internet-based communications, with most solutions relying on sophisticated cryptography techniques.

Although there are a range of legal issues implicated by electronic commerce, the concern that has generated the most attention is that such electronic transactions will run afoul of many laws requiring written records and/or signed records in order for such transactions to have binding legal effect.[7] Writing requirements imposed by law can range from basic contract requirements (e.g., the statute of frauds), to more complex issues (e.g., notarization and attestation). Although opinions differ on the proper scope and substance of legal reforms which might be needed,[8] most electronic commerce legislation to date has addressed the issue of electronic signatures.[9]

TECHNOLOGY PRIMER

There are many methods for creating an electronic signature. These methods range from simple ones, such as typing a name at the bottom of an e-mail message, to more complex and secure ones, involving biometric technologies, such as fingerprint or retinal scans. Other types of authentication methods used to create electronic signatures include: magnetic stripe cards with personal identification numbers (PIN), user names and passwords, public-key cryptography, writing tablets with electronic pens, and even smart cards that generate a unique access code every few seconds. As technology advances, the list of viable electronic signature alternatives is certain to grow.

Because there are so many methods for creating an electronic signature, and because many of them do not resemble a holographic ``autograph,'' many law reform efforts have adopted the term ``authentication'' rather than ``signature.'' For example, the current drafts of Uniform

Commercial Code (U.C.C.) Articles 2 and 2B eliminate the term ``sign'' and instead allow the authenticity of documents to be proven in any reasonable manner.[10] These drafts also clarify that assent may be manifested through any form of authentication, including proof of the authentication process itself.[11]

One of the most interesting and robust technologies being used and developed for authentication purposes is known as public-key cryptography, which allows for a very high degree of reliability when implemented properly. A ``digital signature'' does not refer to the image of a signature in any way. Unlike both an ``electronic signature,'' which is simply any form of mark intended to be a signature, and a ``digitized signature,'' which refers to an electronic image of a signature, a ``digital signature'' is actually a term of art that refers to scrambling data in order to provide security and authentication.[12] Although the technical details of public-key cryptography are extremely complex and of limited utility to a broader audience, an understanding of the basic concepts is both accessible and useful. Due to the current interest in deploying large scale public-key systems, it is likely that this technology will touch many areas of the economy. In fact, the growth of public-key systems in many sectors of the economy suggests that a rudimentary knowledge of these concepts will serve lawyers well when legal questions arise in the context of this technology.

THE BASICS OF PUBLIC-KEY CRYPTOGRAPHY[13]

Codes and cryptography are thousands of years old. Although cryptography has become much more sophisticated in modern times, it still relies on both the sender and the receiver knowing the same ``secret key'' to encode and then decode messages. To be secure, a secret-key coding system requires some method for distributing the secret key to intended users without it

falling into the hands of other parties.

By its nature, the Internet is poorly suited for a secret-key system because it is an ``open'' network in which a message may make several ``stops'' before arriving at its final destination. This creates a serious risk that a third party could intercept a secret key at some point along its routing, which would allow the third party to read messages, or even send encoded messages purporting to be from the authorized holder of a secret key. Physically delivering a secret key to every user through a secure channel would be slow, expensive, and unwieldy. It would effectively rule out serendipitous or one-time transactions between people and firms that have not previously exchanged secret keys.

Public-key cryptography eliminates the need for users to share a secret key, which makes it ideally suited for communications over open networks such as the Internet. The hardware and software that implements this technology shields the end user from the details of the following complex illustration; end users do not need to know about the complicated background operations that make the system possible.

In a public-key system, each user has software that generates two related keys, a public key and a private key. The fundamental characteristic of this key pair is that only this particular public key can decrypt a message encrypted by its corresponding private key. Similarly, only this particular private key can decrypt a message encrypted by its corresponding public key. As such, these key pairs are analogous to secret decoder rings from a box of cereal--each ring fits into its companion ring and no other.[14]

For example, once Bob, a public-key system user, has generated his public/private-key pair with a computer, he keeps his private key very secure (i.e., protected by a password on his computer or, preferably, on a smart card locked in a safe), but he makes his public key freely available by sending it to other public-key system users, or by posting it to a public-key directory

on the Internet. Then, if Alice, another public-key system user, wants to send Bob a private message, she can obtain Bob's public key and use it to encrypt the message. Because only Bob's private key can decrypt a message that has been encrypted with his public key, both Alice and Bob can be sure that only Bob can read the message. Thus, public-key cryptography allows two people to send secure messages without the need to exchange a secret key through a secure channel. Only Bob's public key needs to be shared in order for Bob to receive completely secure messages.

INSERT DIAGRAM HERE

This unique characteristic of public-key cryptography also forms the basis for secure digital signatures. This process is illustrated in the diagram. In order to generate a digital signature, Bob must first have a message (1) that he wants to sign and send to Alice. It could be as simple as an e-mail message or as complicated as a lengthy contract. Bob would then run his communication to Alice through one of several standard algorithms, known as a hash function (2) that performs a series of mathematical operations on the original message. The hash function produces a number, called a message digest (3) that can be thought of as a fingerprint of the message because any change in the message, no matter how slight, will cause the hash function to produce a completely different message digest. Bob would then encrypt the message digest with his private key (4). The message digest encrypted with Bob's private key forms the actual digital signature for the message.[15] Finally, Bob would transmit both the digital signature and his original message to Alice (5). If Bob also wants to keep his message to Alice confidential, he could encrypt the message using Alice's public key.

Upon receipt, Alice's computer and software would perform two separate operations to

verify Bob's identity and determine if the message had been altered in transit. As a practical matter, it is not important which operation is performed first.[16] To verify Bob's identity, Alice's system would take Bob's digital signature (1) and then use Bob's public key (2) to decrypt the digital signature, which will produce the message digest (3). If this operation is successful, Alice knows for a fact that Bob, who alone has access to his private key, must have sent the message.

In order to ensure that Bob's message had not been altered in transit, Alice would run Bob's message (4) through the same hash function (5) that Bob used, which would yield a message digest of Bob's message (6). Alice would then compare the two message digests (7), and, if they were the same, she would know for a fact that the message had not been altered in transit.

Thus, public-key cryptography allows people and businesses to exchange messages over open networks with a high degree of confidence that those messages are confidential (i.e., unable to be read by unauthorized persons), authentic (i.e., the sender's identity can be verified), and accurate (i.e., the message cannot be altered without detection). This is a level of security far greater than that afforded by ink signatures. This technology can enable the use of online systems to send and receive tax returns, purchase orders, mortgage applications, credit card orders, and any other type of sensitive or official information with greater security than if the transactions were conducted on paper.

Nothing mentioned so far rules out the possibility, however, that an impostor could generate a public/private-key pair and then post the public key on the Internet claiming that it belongs to Bob. Unaware of the deception, Alice might then use this public key to send messages that the impostor, but not Bob, could read. The impostor can also use the fake private key to digitally sign messages that Alice would assume Bob sent because they can be decoded using the public key that Alice does not yet realize is fraudulent. In order to prevent this, parties

relying on digital signatures must have confidence that a public key on the Internet which purports to belong to Bob is, in fact, owned by him. A trusted third party, known as a certification authority (CA), performs this function.

A CA binds the identity of a particular party to a particular public key and, by implication, a particular private key. CA's do this by issuing a digital certificate. A digital certificate is a small electronic record that (i) identifies the issuing CA, (ii) identifies the subscriber, (iii) contains the subscriber's public key, and (iv) bears the digital signature of the CA's private key. The digital certificate can also contain additional information, including a reliance limit or a reference to the CA's ``certification practice statement'' that gives relying parties notice of the level of inquiry conducted by the CA before issuing the certificate.

To obtain a digital certificate, Bob presents the CA with a copy of his public key along with sufficient proof of his identity. For digital certificates in larger transactions, the CA might charge a higher fee and require greater proof of identity. Once satisfied as to the identity of the subscriber, the CA issues the subscriber a digital certificate. When Bob wants to use his digital signature, he transmits a copy of his digital certificate to Alice. In addition to the steps described above, upon receipt of Bob's message, Alice's computer also confirms with the CA identified in the digital certificate that Bob is who he purports to be and that his certificate has not expired or been revoked. If Bob learns or fears that his private key has been compromised, he notifies his CA so that it will post that information to its ``certificate revocation list.'' All of this activity takes place in the background, unseen and unnoticed by Alice, and happens in much the same way as it occurs with online credit-card validation systems.

One of the major unanswered questions about the use of public-key cryptography for digital signatures, and a major point of contention between advocates of different types of electronic signature laws, relates to the business model for CA services that will ultimately

prevail in the marketplace. A Public Key Infrastructure (PKI) must evolve to support this technology.[17] Although advances in technology will certainly create new possibilities, the two primary business models currently vying for support are known as the ``open PKI'' and ``closed PKI'' models.

An open PKI model assumes that subscribers obtain a digital certificate from a CA that will securely link their identity to their public key for all, or at least many, purposes. Thus, in an open PKI environment, a person could obtain a digital certificate and then use it for a transaction requiring a digital signature, including to order goods online from various merchants, sign legally binding agreements, and even file documents with a government entity.

In the closed PKI model, users obtain a different digital certificate for each online community of interests. For example, a closed PKI user could have one certificate for transactions with a bank, a different certificate for communications with an employer, and yet another certificate for dealings with a health care provider.

The difference between the two models is significant. Under an open PKI model, a person's certificate would potentially sign any document, which yields extremely severe consequences if the user's private key is compromised. In a closed PKI, on the other hand, the risks of a fraudulently signed document are more limited because of the system's more narrowly defined scope. Furthermore, the members of a particular community within a closed PKI system may enter into agreements defining the rights and responsibilities of the members, which would allow the parties to further reduce uncertainty and allow the parties to allocate risk.

LEGLISLATION

Although there are a number of federal and international initiatives,[18] states have taken

the lead on electronic commerce and electronic signature legislation.[19] State legislation relating to electronic signatures can be divided into two broad categories: electronic signature legislation and secure signature legislation.[20]

Electronic signature legislation provides that any symbol or method, regardless of the particular technology used, can create a valid signature if executed or adopted by a party with a present intent to be bound.[21] Within this general category of legislation, there are a variety of definitions for the term ``electronic signature.''[22] For example, the Rhode Island Electronic Signatures and Records Act defines an electronic signature as ``an electronic identifier, created by a computer, and intended by the party using it to have the same force and effect as the use of a manual signature.''[23] In Florida, an electronic signature is defined to be ``any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing.''[24]

Secure signature legislation, on the other hand, confers legal validity on a subset of possible electronic signatures regarded as sufficiently secure to warrant favorable legal treatment. There are two primary types of secure signature legislation. The first type, commonly known as digital signature legislation, requires the use of public-key cryptography[25] to create a digital signature.[26] This type of legislation was first enacted by Utah and has been copied by several other states. The Utah act defines a digital signature as:

=xta transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether: (a) the transformation was created using the private key that corresponds to the signer's public key; and (b) the message has been altered since the transformation was made.[27]

Digital signature statutes based on the Utah approach also confer regulatory authority on a state agency to license CAs that operate within their jurisdiction.[28] Licensed CAs that comply with

the requirements of the governing statute are then afforded significant limitations on liability.[29] Moreover, for a digital signature to gain an evidentiary presumption under these statutes, the digital signature must have a verifiable certificate issued from a certification authority licensed under the regulations.[30]

The second type of secure signature legislation does not specify a particular technology. Instead, it establishes certain information security attributes that an electronic signature must possess in order to receive the benefits provided by the statute.[31] California was the first state to adopt this type of legislation and several other states have followed this general approach.[32] The California act states:

[A] digital signature shall have the same force and effect as the use of a manual signature if and only if it embodies all of the following attributes:

(1) It is unique to the person using it.

(2) It is capable of verification.

(3) It is under the sole control of the person using it.

(4) It is linked to data in such a manner that if the data are changed, the digital signature is invalidated.

(5) It conforms to regulations adopted by the Secretary of State.[33]

Statutes of this type generally confer authority on a state agency to promulgate regulations to define what technology and practices shall meet those standards.[34] The State of California has published this type of draft regulations for public comment.[35] Those draft regulations permit the use of two technologies: (i) asymmetric cryptosystems and (ii) a method known as security dynamics, which captures biometric information obtained from the manual signing process on an

electronic pad.[36] California's draft regulations provide a process whereby additional technologies may be added to an approved list, if those technologies meet the standards set by statute and regulation.[37]

In addition to categorizing state legislation into electronic signature laws and secure signature laws, it is also useful to distinguish between statutes based on the scope of transactions to which they apply. Some state statutes apply only to electronic communications with the government.[38] Such statutes apply to any transaction with a state government entity,[39] more narrowly target transactions with a particular department, or cover only specific types of transactions with state government.[40] Broader electronic signature laws apply to both the public and private sectors.[41] Legislation of this type is essential to promote electronic commerce between private parties.[42] Many statutes also specify areas of law or particular sets of transactions as exempt from the scope of the legislation.[43]

Most types of electronic signature legislation provide for the evidentiary treatment of electronic signatures and electronic records.[44] In general, evidentiary provisions address the admissibility of electronic documents[45] and their evidentiary weight.[46] Statutes that specify the evidentiary weight of an electronic signature also presume that a secure signature is that of the person to whom it correlates and that person affixed it with the intention of signing the electronic record.[47] Such an approach risks inequitable results for a consumer who is the innocent victim of a skilled hacker/forger who compromises a secure system. Proponents of such provisions, however, maintain that certain systems, if sufficiently secure, deserve the benefit of an evidentiary presumption and that such presumptions can reduce unnecessary litigation. Beyond the consumer protection issues raised by such a presumption, the process by which parties will prove security is currently undetermined.[48] Ironically, this ensuing battle over such a presumption could increase litigation.

COMPARISON OF UNCITRAL, MASSACHUSETTS, AND NCCUSL STATUTES

The following table provides a side-by-side comparison of some of the major provisions of the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce,[49] the Massachusetts Electronic Records and Signature Act (November 4, 1997, draft),[50] and the National Conference of Commissioners on Uniform State Law (NCCUSL) Uniform Electronic Transactions Act (November 25, 1997, draft).[51] Specifically, this table compares the approaches taken in (i) purpose, (ii) scope, (iii) exclusions from scope, (iv) selected definitions, (v) records, (vi) signatures, (vii) originals, (viii) evidence, (ix) retention, (x) variation by agreement, and (xi) use by state agencies. This comparison exemplifies the current statutory trend in scope, approach, and language.

UNCITRAL	NCCUSL	MERSA

Article 3. Interpretation (1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith. (2) Questions concerning matters governed by this Law that are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.	Section 106. Application and Construction This [Act] must be liberally construed and applied consistently with commercially reasonable practices under the circumstances and to promote its underlying purposes and policies. [purposes found in commentary to section 106] The underlying purposes and policies of this Act are (a) to facilitate and promote commerce and governmental transactions by validating and authorizing the use of electronic records and electronic signatures; (b) to eliminate barriers to electronic commerce and governmental transactions resulting from uncertainties relating to writing and signature requirements; (c) to simplify, clarify, and modernize the law governing commerce and	Section 2. Purposes and Construction The provisions of this Act shall be construed: (a) to facilitate and promote electronic commerce and online government by clarifying the legal status of electronic records and electronic signatures in the context of writing and signing requirements imposed by law; (b) to permit and encourage the continued expansion of electronic commerce and online government through the operation of free market forces rather than proscriptive legislation; (c) to promote public confidence in the validity, integrity, and reliability of electronic commerce and online government; and (d) to promote the development of the legal and business infrastructure necessary to support and encourage electronic

	transactions through the use of electronic means; (d) to permit the continued expansion of commercial and governmental electronic practices through custom, usage, and agreement of the parties; (e) to promote uniformity of the law among the states (and worldwide) relating to the use of electronic and similar technological means of effecting and performing commercial and governmental transactions; (f) to promote public confidence in the validity, integrity, and reliability of electronic commerce and governmental transactions; and (g) to promote the development of the legal and business infrastructure necessary to implement electronic commerce and governmental transactions.	and online government.

DEFINITIONS

UNCITRAL	NCCUSL	MERSA

Article 2. Definitions For the purposes of this Law: (a) ``Data message'' means information generated, sent, received, or stored by electronic, optical, or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex, or telecopy; (b) ``Electronic data interchange (EDI)'' means the electronic transfer from computer to computer of information using an agreed standard to structure the information; (c) ``Originator'' of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message; (d) ``Addressee'' of a data message means a person who is intended by	Section 102. Definitions In this [Act]: (1) ``Agreement'' means the bargain of the parties in fact as found in their language or inferred from other circumstances, including course of performance, course of dealing and usage of trade as provided in this [Act]. Whether an agreement has legal consequences is determined by this [Act], if applicable or, otherwise, by other applicable rules of law. (2) ``Automated transaction'' means a commercial or governmental transaction formed or performed, in whole or in part, by electronic records in which the records of one or both parties will not be reviewed by an individual as an ordinary step in forming a contract, performing under an existing contract, or fulfilling any obligation required by the transaction. (3) ``Commercial	Section 65. Definitions As used in Sections 65-72, the following words shall have the following meanings: ``Electronic'' means electrical, digital, magnetic, optical, electromagnetic, or any other technology that is similar to these technologies. ``Electronic Record'' means a record generated, communicated, received, or stored by electronic means. ``Electronic Signature'' means any identifier or authentication technique attached to or logically associated with an electronic record that is intended by the person using it to have the same force and effect as a manual signature. ``Record'' means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. ``Rule of

originator to receive the data message, but does not include a person acting as an intermediary, with respect to that data message; (e) ``Intermediary,'' with respect to a particular data message, means a person who, on behalf of another person, sends, receives, or stores that data message or provides other services with respect to that data message; and (f) ``Information system'' means a system for generating, sending, receiving, storing, or otherwise processing data messages.	transaction'' means all matters arising in a commercial setting, whether contractual or not, including but not limited to the following: any trade transaction for the supply or exchange of goods, information, or services; distribution agreements; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation or organization; carriage of goods or passengers by air, sea, rail, or road. (4) ``Computer Program'' means a set of statements or instructions to be used directly or indirectly to operate an information system in order to bring about a certain	Law'' means a statute, regulation, ordinance, common-law rule, court decision, or other law relating to a governmental transaction enacted, established, or promulgated by the Commonwealth or any agency, commission, department, court, other authority, or political subdivision of the Commonwealth.

	communicated as a result of the operation of the system. (5) ``Contract'' means the total legal obligation that results from the parties' agreement as affected by this [Act] and as supplemented by other applicable rules of law. (6) ``Electronic'' means electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies. (7) ``Electronic Agent'' means a computer program or other electronic or automated means used, selected, or programmed by a person to initiate or respond to electronic records or performances in whole or in part without review by an individual. (8) ``Electronic record'' means a record created, stored, generated, received, or communicated by electronic means, such as computer	

	equipment and programs, electronic data interchange, electronic or voice mail, facsimile, telex, telecopying, scanning, and similar technologies. (9) ``Electronic Signature'' means any signature in electronic form, attached to or logically associated with an electronic record, executed or adopted by a person or its electronic agent with intent to sign the electronic record. (10) ``Good Faith'' means honesty in fact and the observance of reasonable commercial standards of fair dealing. (11) ``Governmental Transaction'' means all matters arising in any governmental setting, including but not limited to the following: all communications, filings, reports, commercial documentation, or other electronic records relating to interactions between any governmental entity	

	the government; and all intragovernmental communications, documents, or other records employed in the conduct of governmental functions between or within any branch or agency of government. (12) ``Information'' means data, text, images, sounds, codes, computer programs, software, databases, and the like. (13) ``Information System'' means a system for creating, generating, sending, receiving, storing, or otherwise processing information, including electronic records. (14) ``Notify'' means to communicate or make available information to another person in a form and manner as appropriate or required under the circumstances. (15) ``Organization'' means a person other than an individual. (16) ``Person'' means an individual,	

	liability company, association, joint venture, government, subdivision, agency, or instrumentality, or any other legal or commercial entity. (17) ``Presumption'' or ``presumed'' means that the trier of fact must find the existence of the fact presumed unless and until evidence is introduced that would support a finding of its non-existence. (18) ``Record'' means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. (19) ``Rule of Law'' means a statute, regulation, ordinance, common-law rule, court decision, or other law relating to commercial or governmental transactions enacted, established, or promulgated by this State, or any agency, commission, department, court, other authority, or political	

	of this State. (20) ``Security Procedure,'' with respect to either an electronic record or electronic signature, means a commercially reasonable procedure or methodology, established by law, by agreement, or adopted by the parties for the purpose of verifying (i) the identity of the sender or source of an electronic record, or (ii) the integrity of, or detecting errors in, the transmission or informational content of an electronic record. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback, or other acknowledgement procedures, or any other procedures that are reasonable under the circumstances. (21) ``Signature'' means any symbol, sound, process, or encryption of a record in whole	

	adopted by a person or the person's electronic agent with intent to (i) identify the party; (ii) adopt or accept a term or a record; or (iii) establish the informational integrity of a record or term that contains the signature or to which a record containing the signature refers. ``Sign'' means the execution or adoption of a signature by a person or the person's electronic agent. (22) ``State Agency'' means any executive[, legislative or judicial] agency, department, board, commission, authority, institution, or instrumentality of this State or of any county, municipal, or other political subdivision of this State. (23) ``Term'' means that portion of an agreement that relates to a particular matter. (24) ``Transferrable Record'' means a record, other than a writing, that is	

	Article 9 of the [Uniform Commercial Code] or a document of title under Article 1 of the [Uniform Commercial Code]. (25) ``Writing'' includes printing, typewriting, or any other intentional reduction to tangible form. ``Written'' has a corresponding meaning.	

SCOPE AND EXCEPTIONS FROM SCOPE

UNCITRAL	NCCUSL	MERSA

Article 1. Sphere of Application* This Law** applies to any kind of information in the form of a data message used in the context*** of commercial**** activities. *The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages: ``This Law applies to a data message as defined in Paragraph (1) of Article 2 where the data message relates to international commerce." **This Law does not override any rule of law intended for the protection of consumers. ***The Commission suggests the following text for States that might wish to extend the applicability of this Law: ``This Law applies to any kind of information in the form of a data message, except in the following situations:	Section 103. Scope Except as otherwise provided in Section 104 or any regulation adopted pursuant to Part 5, this [Act] applies to electronic signatures generated, stored, processed, communicated, or used for any purpose in any commercial or governmental transaction.	Section 66. Scope (a) Sections 65-72 shall apply to records generated, stored, processed, communicated, or used for any purpose by or with a public entity of the Commonwealth. The provisions of Sections 65-72 shall not apply: (i) to the extent that their application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the lawmaking body or repugnant to the context of the same rule of law, provided that the mere requirement that information be ``in writing," ``written," ``printed," or ``signed," or any other word that purports to specify or require a particular communications medium, shall not by itself be sufficient to establish such intent; or (ii) to any record that serves as a unique

[. . .]." ****The term ``commercial'' should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include but are not limited to the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road. [Note: Several articles, including	Section 104. Transactions Subject to Other Law (a) This [Act] does not apply to the extent that its application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the lawmaking body or repugnant to the context of the same rule of law, provided that the mere requirement that information be ``in writing,'' ``written,'' ``printed,'' ``signed,'' or any other word that specifies or requires the use of a particular medium of presentation, communication, or storage, shall not, by itself, be sufficient to establish such intent. (b) A transaction subject to this [Act] is also subject to: (1) any applicable rules of law relating to consumer protection; (2) the Uniform Commercial Code as enacted in	and transferrable physical token of rights and obligations including, without limitation, negotiable instruments and other instruments of title wherein possession of the instrument is deemed to confer title. (b) Nothing in Sections 65-72 shall be construed to require any public entity of the Commonwealth to use or permit the use of electronic records or electronic signatures. [Note: The provisions of Section 4 (see the ``Records'' section of this matrix) apply to private sector contracts between business entities. The provisions of Section 5 (see also the ``Records'' section) apply to the definitions section of the Massachusetts General Laws and, hence, have a wide scope.]

with writing and signature requirements, end with the following section: ``The provisions of this article do not apply to the following: [. . .]." The substantive exceptions, if any, would be left to the enacting state to determine.]	[such other rules of law as may be designated at the time of the enactment of this [Act]]. (c) The provisions of this [Act] and a rule of law referenced in subsection (a) or (b) must be construed whenever reasonable as consistent with each other. If such a construction is unreasonable, a rule of law referenced in subsection (a) or (b) governs.	

RECORDS

UNCITRAL	NCCUSL	MERSA

Article 5. Legal Recognition of Data Messages Information shall not be denied legal effect, validity, or enforceability solely on the grounds that it is in the form of a data message.	Section 401. Formation and Validity (a) If an electronic record is used in the formation of a contract, the contract may not be denied legal effect, validity, or enforceability on the sole ground that an electronic record was used for that purpose. (b) Operations of electronic agents that confirm the existence of a contract or signify agreement may form a contract even if no individual was aware of or reviewed the operations. (c) In an automated transaction, the following rules apply . . . (d) If an electronic record initiated by a party or an electronic agent evokes an electronic record in response and the records reflect an intent to be bound, a contract exists when: (1) the response signifying	Section 4. Use of Electronic Records and Electronic Signatures by Business Entities . . . (a) 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 been signed with an electronic signature. For purposes of this section, ``contract'' shall mean a contract for the sale of goods or services, for the sale or license of digital information, or for the lease of tangible personal property. The provisions of this subsection shall not apply to the extent that their application would involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the lawmaking body or repugnant to the context of the same rule of

Article 6. Writing (1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference. (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.	received; or (2) if the response consists of electronically performing the requested consideration in whole or in part when the requested consideration to be performed electronically is received, unless the originating record prohibited that form of response. 30	law, provided that the mere requirement that information be ``in writing,'' ``written,'' ``printed,'' or ``signed,'' or any other word that purports to specify or require a particular communications medium, shall not by itself be sufficient to establish such intent. (b) Nothing in this section shall be construed to prevent a party from establishing reasonable requirements with respect to the method executed or adopted by a party to sign a contract, absent agreement to the contrary. (c) Nothing in this section shall be construed to mean that electronic records and electronic signatures do not satisfy legal requirements for a writing or a signed writing in transactions not covered by this section.

	31	Section 5. Writings and Signatures Generally Section 7 of Chapter 4 of the General Laws [Note: This is the definitions section] is hereby amended by striking out the thirty-eighth clause and inserting in place thereof the following: ``written'' and ``in writing'' shall include any method, including electronic and digital methods, for inscribing information on a tangible medium or for storing information in an electronic or other medium from which it can be retrieved in perceivable form. In general, where any rule of law purports to specify a particular medium for the creation, storage, communication, or authentication of any records or information, that requirement shall be liberally construed to allow the broadest possible use of electronic

		methods unless there is clear public interest to the contrary.
		=s3Section 67. Electronic Records=s3 [Note: Applies to use of electronic records in or with government] 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.

SIGNATURES

UNCITRAL	NCCUSL	MERSA

Article 7. Signature (1) Where the law requires a signature of a person, that requirement is met in relation to a data message 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. (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature. (3) The provisions of this Article do not apply to the following: [. . .].	Section 301. Legal Recognition of Electronic Signatures (a) A signature may not be denied legal effect, validity, or enforceability solely because it is in the form of an electronic signature. (b) If a rule of law requires signature or provides consequences in the absence of a signature, the rule of law is satisfied with respect to an electronic record if the electronic record includes an electronic signature. (c) A party may establish reasonable requirements regarding the method and type of signatures that will be acceptable to it.	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. [Note: Applies to use of electronic records in or with government] [Note: See also Section 4 and Section 5 in the ``Writings'' section of this matrix]

	Section 302. Electronic Signatures: Effect and Proof (a) Unless the circumstances otherwise indicate that a party intends less than all of the effect, an electronic signature is intended to establish (1) the signing party's identity, (2) its adoption and acceptance of a record or a term, and (3) the informational integrity of the record or term to which the electronic signature is attached or with which it is logically associated. (b) If the signing party executed or adopted the electronic signature in accordance with a security procedure, the electronic record to which the electronic signature is attached or with which it is logically associated is presumed to be signed by the signing party. Otherwise, an electronic signature may be proven	

	that (1) a procedure existed by which a party must of necessity have signed or manifested assent to a record or term in order to proceed further in the processing of the transaction, or (2) that the party is bound by virtue of the operations of its electronic agent. (c) The authenticity of and authority to make an electronic signature is admitted unless specifically denied in the pleadings. If the validity of an electronic signature is denied in the pleadings, the burden of establishing validity is on the person claiming validity.	

	Section 303. [Signatures by] [Operations of] Electronic Agents (a) A party that designs, programs, or selects an electronic agent is bound by operations of its electronic agent. (b) An electronic record resulting from the operations of an electronic agent shall be deemed signed by a party designing, programming, or selecting the electronic agent, regardless of whether the operations result in the attachment or application of an electronic signature to the electronic record.	

EVIDENCE

UNCITRAL	NCCUSL	MERSA

Article 9. Admissibility and Evidential Weight of Data Messages (1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence: (a) on the sole ground that it is a data message; or (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form. (2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which	Section 404. Admissibility Into Evidence (a) In any legal proceeding, the rules of evidence must not be applied to deny the admissibility in evidence of an electronic record or electronic signature: (1) on the sole ground that it is an electronic record or electronic signature; or, (2) on the grounds that it is not in its original form or is not an original. (b) In assessing the evidentiary weight of an electronic record or electronic signature, the trier of fact shall consider the manner in which the electronic record or electronic signature was generated, stored, communicated, or retrieved, the reliability of the manner in which the integrity of the electronic record or electronic signature was maintained, the manner in which	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. [Note: Applies to use of electronic records in or with government] [Note: See also Section 4 in the ``Writings'' section of this matrix]

which its originator was identified, and to any other relevant factor.	its originator was identified or the electronic record was signed, and any other relevant information or circumstances.	

ORIGINALS

UNCITRAL	NCCUSL	MERSA

Article 8. Original	Section 204. Originals: Information Accuracy	Section 70. Originals
(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if: (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented. (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form. (3) For the purposes of	(a) If a rule of law [or a commercial practice] requires a record to be presented or retained in its original form, or provides consequences for the record not being presented or retained in its original form, that requirement is met by an electronic record if [the electronic record is shown to reflect accurately] [there exists a reliable assurance as to the integrity of] the information set forth in the electronic record from the time when it was first generated in its final form, as an electronic record or otherwise. (b) The integrity and accuracy of the information in an electronic record are determined by whether the information has remained complete and unaltered, apart from the	If a rule of law requires a record to be presented or retained in its original form or provides consequences for the record not being presented or retained in its original form, that requirement is met by an electronic record if it accurately reproduces the original record as it existed at the time in question.

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage, and display; and (b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances. (4) The provisions of this Article do not apply to the following: [. . .].	change that arises in the normal course of communication, storage, and display. The standard of reliability required must be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.	

RECORDS RETENTION

UNCITRAL	NCCUSL	MERSA

Article 10. Retention of Data Messages	Section 205. Retention of Electronic Records	Section 71. Retention of Electronic Records
(1) Where the law requires that certain documents, records, or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied: (a) the information contained therein is accessible so as to be usable for subsequent reference; (b) the data message is retained in the format in which it was generated, sent, or received, or in a format that can be demonstrated to represent accurately the information generated, sent, or received; and (c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received. (2) An obligation to	(a) If a rule of law requires that certain documents, records, or information be retained, that requirement is met by retaining electronic records, if: (1) the information contained in the electronic record remains accessible so as to be usable for subsequent reference; (2) the electronic record is retained in the format in which it was generated, stored, sent, or received, or in a format that can be demonstrated to reflect accurately the information as originally generated, stored, sent, or received; and (3) the information, if any, is retained as enables the identification of the source of origin and destination of an electronic record and the date and time it was sent or received.	If a rule of law requires that a record be retained, that requirement is met by retaining an electronic record if it accurately reproduces the original record as it existed at the time in question and for so long as may be required by law. Nothing in this section shall preclude any federal or state agency from specifying additional requirements for the retention of records, either written or electronic, that are subject to the jurisdiction of such agency.

or information in accordance with Paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received. (3) A person may satisfy the requirement referred to in Paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b), and (c) of Paragraph (1) are met.	documents, records, or information in accordance with subsection (a) does not extend to any information the sole purpose of which is to enable the record to be sent or received. (c) A person may satisfy the requirement referred to in subsection (a) by using the services of any other person, if the conditions set forth in subsection (a) are met. (d) Nothing in this section precludes any federal or state agency from specifying additional requirements for the retention of records, either written or electronic, subject to the agency's jurisdiction.	

PERMISSIVE

UNCITRAL	NCCUSL	MERSA

Article 4. Variation by Agreement (1) As between parties involved in generating, sending, receiving, storing, or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement. (2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.	Section 105. Variation By Agreement (a) As between parties involved in generating, storing, sending, receiving, or otherwise processing or using electronic records or electronic signatures, the provisions of this [Act] may be varied by agreement, except: (1) the obligations of good faith, reasonableness, diligence, and care prescribed by this [Act] may not be disclaimed by agreement but the parties may by agreement determine the standards by which the performance of such obligations is to be measured if such standards are not manifestly unreasonable; and (2) the rules in Section 110 regarding allocations of loss where no security procedure or commercially unreasonable security procedures are used in a transaction. (b) The	[This Act does not attempt to change or clarify substantive contract law and, therefore, requires no such clause.]

	``unless otherwise agreed'' or words of similar import does not imply that the effect of other provisions may not be varied by agreement under subsection (a). (c) This [Act] does not require that records or signatures be generated, stored, sent, received, or otherwise processed or used by electronic means or in electronic form.	

GOVERNMENTAL

UNCITRA:	NCCUSL	MERSA

	Section 501. Use of Electronic Records by State Agencies (a) [Except where expressly prohibited by statute,] Every state agency may create and retain electronic records in place of written records and may convert written records to electronic records. [The [designated state officer] shall issue rules governing the disposition of written records after conversion to electronic records.] (b) Any state agency that accepts the filing of records or requires that records be created or retained by any person, may authorize the filing, creation, or retention of records in the form of electronic records [except where expressly prohibited by statute]. (c) In any case governed by subsection (a) or (b), the state agency, by appropriate regulation	Section 3. Electronic Records and Signatures . . . 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,

	to security, [may] [shall] specify: (1) the manner and format in which the electronic records must be filed, created, or retained; (2) if electronic records must be electronically signed, the type of electronic signature required, and the manner and format in which the electronic signature must be affixed to the electronic record; (3) control processes and procedures as appropriate to ensure adequate integrity, security, confidentiality, and auditability of electronic records; and (4) any other required attributes for electronic records that are currently specified for corresponding non-electronic records. (d) In establishing regulations under subsection (c) state agencies shall give due regard to regulations implemented by other state agencies, other states, and the federal government for	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. Section 70. Originals. If a rule of law requires a record to be presented or retained in its original form, or provides consequences for the record not being presented or retained in its original form, that requirement is met by an electronic record if it accurately reproduces the original record as it existed at the time in question. Section 71. Retention of Electronic Records. If a rule of law requires that a record be retained, that requirement is met be retaining an electronic record if it

	conflicting regulations that would impede commerce and the implementation of electronic transactions. (e) Nothing in this [Act] may be construed to require any state agency to use or permit the use of electronic records or signatures.	reproduces the original record as it existed at the time in question and for so long as may be required by law. Nothing in this section shall preclude any federal or state agency from specifying additional requirements for the retention of records, either written or electronic, that are subject to the jurisdiction of such agency. Section 72. Role of the Chief Information Officer. The Chief Information Officer designated in Section 4-A of Chapter 7 shall have the authority to coordinate, oversee, operate, and approve the use of information security and authentication technologies by any public entity within the executive department.

As the table demonstrates, some standardization in language is emerging. The NCCUSL committee drafting the Uniform Electronic Transactions Act is serving as a very important forum for states and other stakeholders that are endeavoring to craft appropriate legislation. It is important to note that consistency among state laws in this field is a highly relevant factor for federal legislators and regulators who will decide whether, when, and to what extent federal preemption of state action will occur. Ultimately, there will be a role for state, federal, and international law. Traditional state areas of jurisprudence (e.g., contract law, commercial law, and state rules of evidence) should continue to be respected as the nation moves toward an information age. Development of uniform state law is critical to the smooth evolution of electronic commerce and online government applications in the years to come.

POLICY CONTEXT OF ELECTRONIC COMMERCE LEGISLATION

Advocates of proscriptive legislation, such as that adopted by Utah, Washington, and Minnesota, believe that digital signatures based on public-key cryptography represent a nearly ideal technical solution to the problem of authenticating Internet transactions. These advocates, therefore, believe legislation must first be adopted to address these issues before such signatures are widely used. First, digital signatures must be given the same legal force as traditional signatures.[52] Second, CAs need to be licensed by the state in order to ensure that they are technically proficient, financially sound, and operationally secure. In addition, legislation is needed to shield CAs from potentially crippling liability if they have complied with requirements established by law.

Advocates of this type of statute believe that proactive legislation is preferable to

allowing the validity of digital signatures to be determined by the evolution of the common law, technical standards, and business practices in the market. They also believe this legislation is more likely to produce uniformity among different jurisdictions, not only on a state or federal level, but internationally as well. With this legal infrastructure in place, they believe electronic commerce will gain broader acceptance because parties to online transactions will be able to use digital signatures that are secure and legally enforceable.

Although legislation based on the Utah model has many vigorous proponents, there are a number of policy issues raised by this approach. Critics of the Utah legislation believe that proscriptive, technology-specific legislation runs the risk of distorting the market, thus preventing the natural evolution of the best business practices, technological innovations, and competitive pricing.[53] Many observers believe that detailed statutory and regulatory treatment is simply inappropriate in an infant industry undergoing rapid change. In the Telecommunications Act of 1996, Congress expressly found that ``[t]he Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation"[54] and declared that ``[i]t is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."[55]

This nonregulatory environment has allowed the Internet to evolve solely in response to advances in technology, the creativity of providers, and the needs of users, rather than in conformance with detailed strictures laid down by government bureaucrats.[56] Freed from government mandates, producers and consumers can quickly and easily adapt to new technologies and business models. This is the dynamic that has caused such explosive growth in the Internet, and it should not be ignored by policy makers when they consider the best ways to promote electronic commerce.

*Daniel J. Greenwood is Deputy General Counsel for the Information Technology Division (ITD) of the Commonwealth of Massachusetts. Mr. Greenwood is Chair of the Online Government Task Force, a multi-agency initiative to bring Massachusetts state government online for citizens and businesses. He is the Governor of Massachusetts' appointed representative to the United States Innovation Partnership, an initiative of the White House and the National Governor's Association to foster cooperation in national technology policy. He also holds an academic appointment as Lecturer at Massachusetts Institute of Technology, where he teaches at the graduate level on topics of electronic commerce and virtual communities. Mr. Greenwood Chairs the Electronic Contracts Work Group of the American Bar Association's (ABA's) Committee on the Law of Commerce in Cyberspace, and he also Chairs the Legislative and Regulatory Work Group of the ABA's Information Security Committee.

Ray A. Campbell is General Counsel for the ITD of the Commonwealth of Massachusetts where he is responsible for providing legal and policy guidance on the state's use of information technology. Before joining ITD, he served as the Director of Special Projects at the Commonwealth's Executive Office for Administration and Finance. Prior to joining state service, Ray worked as an attorney in private practice with the law firm Burns & Levinson, the Bank of New England, and the Bank of Tokyo. He has also worked for the Senate Banking Committee in Washington and the American Institute for Economic Research. He received a B.A. from Bates College in 1982, a J.D. from Suffolk University in 1986, and an M.B.A. from Harvard University in 1991.

Mr. Campbell and Mr. Greenwood thank Suffolk University Law School interns Steve Jensen, Pamela Prieo, and Jon Swartz for their assistance with the production of this Article.

1.*See* Reno v. ACLU, 117 S. Ct. 2329, 2334 (1997) (noting that the number of host computers on the Internet has increased from 300 in 1981 to roughly 9.4 million in 1996).

[2].. The term ``electronic commerce'' has become shorthand for a broad range of transactions that are, or can be, conducted using computer networks, some of which are not necessarily commercial in nature (such as transactions with governments).

[3].. *See* THE FRAMEWORK FOR GLOBAL ELECTRONIC COMMERCE (1997) [hereinafter FRAMEWORK].

[4].. *See*, *e.g.*, CAL. GOV'T CODE § 16.5 (West Supp. 1997); UTAH CODE ANN. §§ 46-3-102 to -501 (Supp. 1997); *Reno*, 117 S. Ct. at 2329; FRAMEWORK, *supra* note 3.

[5].. *See, e.g.*, INFORMATION SEC. COMM., ABA, DIGITAL SIGNATURE GUIDELINES (1996) [hereinafter DIGITAL SIGNATURE GUIDELINES]; M. ETHAN KATSH, LAW IN A DIGITAL WORLD (1995); ONLINE LAW: THE SPA'S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET (Thomas J. Smedinghoff ed., 1996). Congress is also beginning an inquiry into possible federal electronic authentication legislation, and has held hearings under the Domestic and International Monetary Policy Subcommittee of the Committee on Banking and Financial Services of the U.S. House of Representatives. For testimony, see *Witness List for July 9, 1997, Domestic and International Monetary Policy Subcommittee Hearing on Federal Rule in Electronic Authentication* (visited Oct. 20, 1997) <http://www.house.gov/banking/7997wit.htm>.

[6].. MICROSOFT PRESS COMPUTER DICTIONARY 258 (3d ed. 1997).

[7].. Although the statute of frauds is the most common example of a writing requirement, a search of the Massachusetts General Laws reveals over 4500 sections containing one or more of the words ``write,'' ``written,'' ``writing,'' ``sign,'' ``signed,'' and ``signature.'' There are also many sections that use other formulations (such as instrument, document, execute, etc.) not captured by this search. *See generally* HENRY H. PERRITT, JR., LAW AND THE INFORMATION SUPERHIGHWAY (1996); JONATHAN ROSENOER, CYBERLAW: THE LAW OF THE INTERNET (1997); BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE (2d ed. 1996).

[8].. *See, e.g.*, 18 U.S.C. § 1030 (1994) (covering fraud and related activity in connection with computers); *id*. § 1343 (covering fraud by wire, radio, or television); *Reno*, 117 S. Ct. at 2329 (invalidating certain portions of the Communications Decency Act of 1996 as violating free speech and due process).

[9].. *See generally* WARWICK FORD & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE (1997); C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace* (*DRAFT: 5/27/97*) (visited Oct. 20, 1997) <http://www.acusd.edu:80/~biddle/LMW.htm>; C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure* (visited Oct. 20, 1997) <http://www.acusd.edu/~biddle/mp.html>; Legal Dep't, Mass. ITD, *Electronic Signatures and Records: Legislation, Policy and Technology* (visited Oct. 20, 1997) <http://www.magnet.state.ma.us/itd/legal/esigs.htm>; Legal Dep't, Mass. ITD, *Matrix of State Legislation to Date* (visited Oct. 20, 1997) <http://www.magnet.state.ma.us/itd/legal/sigleg7.htm#State Government Electronic and Digital Signature Legislation> [hereinafter *Matrix of State Legislation*].

[10].. U.C.C. § 2B-102(a)(2) (Draft Mar. 21, 1997); *id*. § 2-102(a)(1) (Draft May 16, 1997). According to both the March 21, 1997 draft of section 2B-102(a)(2), and the May 16, 1997 draft of section 2-102(a)(1), the term ``authenticate'' means:

=xt[To] sign or to execute or adopt a symbol, including a digital signal and identifier, or to do an act that to encrypt a record or an electronic message in whole or in part, with present intent to adopt, establish the authenticity of, or signify a party's acceptance and adoption of, a record or term that contains the authentication or to which a record containing the authentication refers.=ft

Id. § 2B-102(a)(2) (Draft Mar. 21, 1997); *id*. § 2-102(a)(1) (Draft May 16, 1997). Reporter's Note 2 of section 2B-102 explains the significance of these changes, stating:

=xtThis article replaces the traditional idea of ``signature'' or ``signed '' with a term that incorporates modern electronic systems, including all forms of encryption or digital symbol systems. Substantive rules on proof of authentication are in Section 2B-[114]. Basically, the fact of authentication can be proved in any manner including proof of a process that necessarily resulted in authentication. Use of an ``attribution procedure'' agreed to by the parties per se establishes that a symbol or act constitutes an authentication.=ft

Id. § 2B-102 Reporter's note 2 (Draft Mar. 21, 1997) (alteration in original).

[11].. *See id*. § 2B-112. According to section 2B-114(b):

=xtA record or message is authenticated as a matter of law if the symbol executed or adopted by a party complies with an attribution procedure for authentication agreed to or adopted by the parties. Otherwise, authentication may be proven in any manner, including by showing that a procedure existed by which a party necessarily must have executed or adopted a symbol in order to proceed further in the use or processing of the information.=ft

Id. § 2B-114(b).

[12].. MICROSOFT PRESS COMPUTER DICTIONARY, *supra* note 6, at 145.

[13].. *See* Legal Dep't, Mass. ITD, *The Basics of Public Key Cryptography and Digital Signatures* (last modified Dec. 19, 1996) <http://www.state.ma.us/itd/legal/crytpo-3.htm>; *see also* William A. Tanenbaum, *Computer Security and Encryption FAQ*, COMPUTER LAW., July 1997, at 19.

[14].. The math underlying public-key cryptography is rather esoteric and is beyond the scope of this paper. In short, public-key cryptography is based on the fact that the only way to factor a large prime product (a very large number derived by multiplying two large prime numbers) is by having a computer calculate every possible combination of numbers in order to find the two component numbers. If the component numbers are large enough, solving the equation becomes ``computationally intractable.'' The current generation of public-key cryptosystems use numbers so large that it would take extremely powerful computers years, and millions of dollars, to crack a single public/private key pair. *See* Tanenbaum, *supra* note 13, at 20.

[15].. The digital signature is created in two distinct steps. First, the message digest, created through the use of a hash function, ensures the integrity of the content of the intended communication. Second, the identity of the person sending the message is authenticated through the use of the private key, which encrypts the message digest. *See id*.

[16].. The two operations are performed upon separate documents; one upon the digital signature, an encrypted message digest, and the other upon the message itself. Although the results of both operations are compared against each other to obtain a true verification, it is irrelevant which operation is performed first. *See id*.

[17].. The acronym PKI stands for Public Key Infrastructure, reflecting the fact that the use of digital signatures based on public-key cryptography requires the support of an elaborate infrastructure (technical, business, policy, and legal). *See*, *e.g.*, Marc Ferranti, *Online Commerce Poses Threat to Banking*, COMPUTERWORLD, Mar. 3, 1997, *available in* 1997 WL 7733293.

[18].. *See*, *e.g.*, UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE, 36 I.L.M. 197 (1997). For a brief overview, see Harold S. Burman, *Introductory Note*, *id*. at 197.

[19].. Utah was the first state to pass such a law. Utah Digital Signature Act, UTAH CODE ANN. §§ 46-3-102 to -501 (Supp. 1997). As of this writing, 14 states have some type of legislation dealing with electronic authentication. *See Matrix of State Legislation*, *supra* note 9.

[20].. Unfortunately, various statutes and texts have mixed definitions. There is a pronounced desire among technical and scholarly legal communities to reserve the term ``digital signature'' for signatures that are created by using public key-based cryptographic systems. The term ``electronic signature'' refers generically to any computer-based technology, including a PIN, a biometric authentication device, a digital signature, etc. The term ``digitized signature'' refers to the digital image of a hand-written signature. *See* DIGITAL SIGNATURE GUIDELINES, *supra* note 5, at 3.

[21].. Under common law, it has been well established that any mark or symbol may create a signature. *See* WRIGHT, *supra* note 7, § 16.2.

[22].. For a more detailed discussion of this point, see Legal Dep't, Mass. ITD, *General Policy Issues* (visited Feb. 16, 1998) <http://www.state.ma.us/itd/legal/genpol.htm>.

[23].. 1997 R.I. Pub. Law, 320, § 1 (to be codified at R.I. GEN. LAWS § 42-127-3(a)).

[24].. FLA. STAT. ANN. § 282.72(4) (West 1996).

[25].. Frequently called ``asymmetric cryptosystems.'' *See* DIGITAL SIGNATURE GUIDELINES, *supra* note 5, at 8.

[26].. MINN. STAT. ANN. §§ 325K.001-.26 (1997); UTAH CODE ANN. §§ 46-3-101 to -504 (Supp. 1997); WASH. REV. CODE ANN. §§ 19.34.010-.903 (West Supp. 1997).

[27].. UTAH CODE ANN. § 46-3-103(10). This definition was also used in bills of other states. *See* MINN. STAT. ANN. § 325K.01(11).

[28].. *See* UTAH CODE ANN. §§ 46-3-201 to -204.

[29].. *Id*. § 46-3-309. The section provides the following liability limitations and reads as follows:

=xt(1) By specifying a recommended reliance limit in a certificate, the issuing certification authority and the accepting subscriber recommend that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit.

(2) Unless a licensed certification authority waives application of this subsection, a licensed certification authority is:

(a) not liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with all material requirements of this chapter;

(b) not liable in excess of the amount specified in the certificate as its recommended reliance limit for either:

(i) a loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed certification authority is required to confirm;

(ii) or failure to comply with Section 46-3-302 in issuing the certificate;

(c) liable only for direct, compensatory damages in any action to recover a loss due to reliance on the certificate, which damages do not include:

(i) punitive or exemplary damages;

(ii) damages for lost profits, savings, or opportunity;

(iii) or damages for pain or suffering.=ft

Id.

[30].. *Id*. § 46-3-406.

[31].. CAL. GOV'T CODE § 16.5 (West Supp. 1997); GA. CODE ANN. §§ 10-12-3 (Supp. 1997); TEX. BUS. & COM. CODE ANN. § 2.108 (19__); TEX. GOV'T CODE ANN. § 2054.060 (West ___); *See also* Commission on Elec. Commerce and Crime, Ill. Office of Attorney Gen., *Illinois Electronic Commerce Security Act* (*IECSA*) (*Draft*) (last modified Sept. 2, 1997) <http://www.mbc.com/ds_stat.html> [hereinafter *IECSA*]; Legal Dep't, Mass. ITD, *Massachusetts Electronic Records and Signature Act* (*MERSA*) (*Draft*) (last modified Sept. 12, 1997) <http://www.magnet.state.ma.us/ifd/legal/mersa.htm> [hereinafter *MERSA*].

[32].. *See* CAL. GOV'T CODE § 16.5; *see also* GA. CODE ANN. §§ 10-12-3; *IECSA*, *supra* note 31, § 302.

[33].. CAL. GOV'T CODE § 16.5(a). It should be noted, however, that not all such statutes require promulgation of regulations. For instance, Georgia's statute merely states the first four standards. GA. CODE ANN. §§ 10-12-3(1). The Georgia statute avoids problems of drafting sound regulations, but creates a lack of certainty as to whether a given technology system meets the statutory requirements.

[34].. CAL. GOV'T CODE § 16.5(a)(5); TEX. GOV'T. CODE ANN. § 2054.060(b). One notable exception to this trend is the Georgia statute. *See* GA. CODE ANN. §§ 10-12-3.

[35].. *See* California Secretary of State, *Text of Proposed Digital Signature Regulations* (visited Oct. 21, 1997) <http://www.ss.ca.gov/digsig/regs.htm>.

[36].. *See id*. § 22003. The proposed regulations deal with signature dynamics in section 22003(b), List of Acceptable Technologies, and are drafted as follows:

=xt[The] technology known as ``Signature Dynamics'' is an acceptable technology for use by public entities in California, provided that the signature is created consistent with the provisions in Section 22003(b)(1)-(5).

1. Definitions--For the purposes of Section 22003(b), and unless the context expressly indicates otherwise:

A. ``Handwriting Measurements'' means the metrics of the shapes, speeds and/or other distinguishing features of a signature as the person writes it by hand with a pen or stylus on a flat surface.

B. ``Signature Digest'' is the resulting bit-string produced when a signature is tied to a document using Signature Dynamics.

C. ``Expert'' means a person with demonstrable skill and knowledge based on training and experience who would qualify as an expert pursuant to California Evidence Code § 720.

D. ``Signature Dynamics'' means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques.

2. California Government Code § 16.5 requires that a digital signature be `unique to the person using it.' A signature digest produced by Signature Dynamics technology may be considered unique to the person using it, if:

A. the signature digest records the handwriting measurements of the person signing the document using signature dynamics technology, and

B. the signature digest is cryptographically bound to the handwriting measurements, and

C. after the signature digest has been bound to the handwriting measurements, it is

[37].. *See id*. § 22004. The California proposal requires the strict usage of CA's to insure the authenticity of digital signatures. The proposal sets forth certain guidelines for CA's to approve and certify. CA's must be on an ``approved list'' and are subject to audits according to AICPA standards. *See id*. § 22004.

[38].. *See* CAL. GOV'T CODE § 16.5(a).

[39].. *Id*.; 1997 Nev. Stat. 249 (codified in scattered sections of NEV. REV. STAT.).

[40].. *See* CONN. GEN. STAT. ANN. § 19a-25a (West 1994) (approving use of electronic signatures for certain medical records); IOWA CODE ANN. § 48A.13 (West Supp. 1997) (dealing only with electronic signatures for voter registration forms).

[41].. FLA. STAT. ANN. §§ 282.70-.75 (West 1996); TEX. BUS. & COM. CODE § 2-108; TEX. GOV'T. CODE ANN. §§ 2054-060 (___); *see* UTAH CODE ANN. §§ 46-3-101 to -504 (Supp. 1997); VA. CODE ANN. § 59.1-467 to -469; (Michie Supp. 1997).

[42].. Although government transactions comprise a large amount of electronic commerce activity, the core of electronic commerce resides with transactions between purely private parties.

[43].. *See*, *e.g*., *MERSA*, *supra* note 31, § 66.

[44].. *See*, *e.g*., UTAH CODE ANN. §§ 46-3-401 to -406 (Supp. 1997); 1997 R.I. Pub. Laws 320, § 1 (to be codified at R.I. GEN. LAWS § 42-127-5).

[45].. The following excerpt from the Rhode Island law exemplifies language that deals purely with admissibility:

=xtIn any legal proceeding, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of an electronic record into evidence on the sole basis that it is an electronic record or that it has been retrieved in perceivable form from an electronic or other medium. An electronic duplicate of a record or any perceivable reproduction of a record that accurately reproduces the original is admissible to the same extent as the original record unless or in the circumstances that it would be unfair to admit the duplicate in lieu of the original.=ft

1997 R.I. Pub. Laws 320, § 1 (to be codified at R.I. GEN. LAWS § 42-127-5).

[46].. Once evidence is admitted, the evidentiary weight requires a distinct analysis.

[47].. MINN. STAT. ANN. § 325K.24 (1997); *see* UTAH CODE ANN. § 46-3-406 (Supp. 1997); WASH. REV. CODE ANN. § 19-34-350 (West Supp. 1997); *see also IECSA*, *supra* note 31, § 303.

[48].. If a litigant has to enlist expert testimony to prove that a secure system was used, then no advantage in reduced litigation efforts would be achieved.

[49].. UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE, 36 I.L.M. 197 (1997).

[50].. *Massachusetts Electronic Records and Signature Act* (Draft) (last modified Nov. 4, 1997) <http://tiac.net/biz/danielg/mersa.htm>.

[51].. UNIF. ELEC. TRANSACTIONS ACT (Draft Nov. 25, 1997) (last modified Nov. 25, 1997) <http://www.law.upenn.edu/library/ulc/vecicta/cct897.htm>.

[52].. Indeed, digital signature legislation typically goes beyond establishing the mere validity of digital signatures by affording evidentiary presumptions in favor of digital signatures certified by a licensed CA.

[53].. For instance, legislation that would limit the liability of certification authorities prevents business people in that sector from crafting business practices to reduce the liability of their companies through more efficient technological implementation and business models. A technical implementation permitting certified third-party reliers to achieve privity with a certificate authority creates an opportunity for those parties to apportion the risks of loss among themselves. The Utah statute envisioned a technical implementation that did not include any contractual privity among third-party reliers on subscriber certificates and the issuing certification authority. *See* David G. Masse & Andrew D. Fernandes, *Economic Modeling and Risk Management in Public Key Infrastructures* (last modified Apr. 15, 1997) <http://www.chait-amyot.ca/docs/pki.html>.

[54].. 47 U.S.C.A. § 230(a)(4) (West 1997).

[55].. *Id*. § 230(b)(2).