Creating Legally Enforceable Electronic Signatures

by George McKenzie



Business people conduct transactions in many ways: a handshake, an e-mail, or a signed contract. Paper-based contracts can be lost or categorized poorly, and citizens are demanding more eco-friendly practices. New business models and trends are also leaning towards electronic forms of transaction documentation due to competitive reasons. This article looks at the legal challenges to executing an electronic signature in the United States.

A typical business transaction usually involves a document, referred to as an "electronic record,"[1] "data message,"[2] or just "record."[3] The documents can also involve an "electronic signature."[4] Increasingly, evidence of these transactions is never actually printed to paper, as the documents reside in an electronic medium: a Hard Disk Drive (HDD), CR ROM, or a tape drive.

Any contract will need to stand up to legal scrutiny for the elements required for a proper contract.[5] The enforceability of electronic signatures raises a host of concerns: whether electronic signatures satisfy requirements imposed by statutes and regulations; whether records maintained solely in an electronic form meet record-keeping requirements; how to establish the authenticity and integrity of such records; their admissibility in court, and others.

The requirement that a document be an "original" occurs in a variety of contexts, from trade documents (e.g., weight certificates, agricultural certificates, or insurance certificates) to birth and death certificates. In many cases, documents must be transmitted unchanged so that other parties may have confidence in their contents. When these documents exist on paper, they are often only accepted as the "original" because alterations may be difficult to detect in a copy. From an evidentiary perspective, the "best evidence rule" (or the "original document rule") requires that: "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress."[6] In many cases, the law requires that a transaction be documented in writing, and be signed by the person who is sought to be held bound, in order for the transaction to be enforceable (e.g., the Statute of Frauds[7]). Some such laws have been interpreted to constitute legal barriers to electronic transactions.[8] This concern about the "legality" of electronic signatures has persisted not only because of a few court decisions, but also, because of a lack of specific legislative authorization.

Legislation

The Federal government, all 50 States, and the governments of at least 55 other countries have enacted some form of legislation on the enforceability and conduct of electronic transactions.[9] In the U.S., the enforceability of electronic transactions is governed by the Electronic Signatures in Global and National Commerce Act (E-SIGN),[10] a federal law enacted in 2000 that largely preempts inconsistent state law, and the Uniform Electronic Transactions Act (UETA),[11] a model state law that was finalized by the National Conference of Commissioners on Uniform State Laws in 1999 and is now adopted by 47 States.[12]

These laws authorize most transactions[13] to be conducted in electronic form.[14] They essentially remove any concerns about the use of electronic signatures, and eliminate inconsistent legal requirements so as to permit electronic commerce to proceed on a uniform legal basis.[15] For example, E-SIGN provides that, notwithstanding any other rule of law, "a signature, contract, or other record relating to [a] transaction... may not be denied legal effect, validity, or enforceability solely because it is in electronic form."[16] UETA provides that "a record or signature may not be denied legal effect or enforceability solely because it is in electronic form"; that "if a law requires a record to be in writing, an electronic record satisfies the law"; and "if a law requires a signature, an electronic signature satisfies the law."[17]

The legislation does not in any way waive the fundamental requirements in the substantive law governing contracts, and there are exceptions to the scope of transactions they authorize. E-SIGN does not apply to wills, family law matters,

court orders, and certain types of written legal notices, and for each state that has adopted UETA or something similar, specific exclusions have been added. Transactions governed by the following laws, or the use of the following documents, are expressly excluded from the scope of E-SIGN, UETA, or both:[18]

- all articles of the Uniform Commercial Code, other than Sections 1-107 and 1-206, and Articles 2 and 2A;
- any document required to accompany the transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials;
- laws governing family law matters, such as adoption or divorce, and laws governing the creation and execution of wills, codicils, or testamentary trusts;
- court orders or notices and other official court documents required to be executed in connection with court proceedings;
- notices of cancellation or termination of utility services;
- notices of default, acceleration, repossession, foreclosure, eviction or of the right to cure, under a mortgage or rental agreement for the primary residence of an individual;

and others.

Which Law Applies?

Both statutes are similar, although there are a number of substantive differences, such as the comprehensive consumer notice and consent requirements that appear in E-SIGN. E-SIGN is a sweeping federal statute that applies to all transactions "in or affecting interstate or foreign commerce,"[19] as defined. Thus, it preempts all inconsistent state laws on such matters. However, E-SIGN contains a provision granting the states the authority to "modify, limit, or supersede the provisions of section 7001"[20] in some circumstances. Section 7001 provides that information relating to a transaction affecting interstate or foreign commerce that is, by law, required to be provided or made available to a consumer in writing, can be made available electronically, if the consumer is first provided with a clear and conspicuous statement disclosing specified information, and consents to receive the information electronically.

This may create a situation where E-SIGN applies to some electronic transactions and UETA applies to others, depending largely on the law enacted in the state whose law will govern the transaction. Moreover, because most of the states that have enacted UETA have made some changes to the official form adopted by NCCUSL, there is a question as to whether these enactments of UETA supersede E-SIGN.

Notice and Consent

UETA is premised on the requirement of consent. The statute will not apply unless the parties have "agreed to conduct transactions by electronic means."[21] This may be either express or implied, and is determined from the context and surrounding circumstances, including the parties' conduct.[22] An express agreement to do business electronically before the transaction is not necessary: if a party goes to a website and enters into a transaction online with the second party, it can arguably be inferred that they have impliedly agreed to conduct the transaction in an electronic form.

Signatures

Signatures can serve a variety of reasons in an electronic transaction. The primary uses for a signature include functioning as a method or device to ensure security (the integrity of the document or to verify its authenticity); providing evidence of intent, in that it shows the signer's intent to enter into the transaction; and to satisfy a law or regulation that requires a signature before the document will be considered legally valid.

Both E-SIGN and UETA build on the concept of an electronic signature. To be an enforceable electronic signature under U.S. law, the electronic signature must contain three elements: a sound, symbol, or process; attached to or logically associated with an electronic record, and made with the intent to sign the electronic record.[23] Electronic signatures that meet these requirements are considered legally enforceable as substitutes for handwritten signatures for most transactions in the U.S.[24]

Although electronic signatures, by their nature, are represented digitally (i.e., as a series of ones and zeroes) they can take many forms, and can be created by many different technologies. Examples of electronic signatures that qualify under E-SIGN and UETA include: a name typed at the end of an e-mail message by the sender; a digitized image of a handwritten signature that is attached to an electronic document (sometimes created using a biometrics-based technology called signature dynamics); a secret code, password, or PIN to identify the sender to the recipient (like those used with ATM cards and credit cards); a unique biometrics-based identifier, such as a fingerprint, voice-print, or retinal scan; a mouse click (the "I accept" button); a sound (e.g., the sound created by pressing "9" on a phone keypad to agree); and a digital signature created using public key cryptography.

This is not an exhaustive list as there are other ways of signing an electronic document, and presumably, many more will be developed in the future. However, all forms of electronic signature must satisfy the three requirements outlined above, in addition to proving that the electronic process has appropriate Information Assurance.[25]

Records Retention

Another key requirement for the enforceability of electronic transactions is that the documents that comprise the

continued on page 26

George McKenzie is the founder of YesDocs.com, an online electronic signature solution. As a software architect with over 20 years of software development experience, his passion to reduce our environmental footprint has helped George to offer a solution to the paper and fax headaches that haunt us today. Paper is a significant source of environmental resource consumption and YesDocs helps reduce paper headaches while speeding up your signature processes. In addition to being green, YesDocs offers a solution that pays for itself in efficiency, cost, and time savings. George resides with his family in beautiful Southern California.

Electronic Signatures *continued from page 25*

transaction be communicated in a form that can be retained and accurately reproduced by the receiving party. The E-SIGN legislation provides that the legal effect, validity or enforceability of an electronic record "may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record."[26] Likewise, UETA provides that "if a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient."[27]

E-SIGN and UETA provide that storage of an electronic record will satisfy legal record retention requirements if the stored copy of the electronic record accurately reflects the information set forth in the record and remains accessible for later reference. E-SIGN and UETA also provide that if a rule of evidence or other rule of law requires a record relating to a transaction to be provided or retained in its original form, this obligation is satisfied by meeting the accuracy and accessibility requirements listed above, so that records can be kept in electronic-only form.

Trust

Beyond the statutory requirements for enforceability, the primary concern of the parties to an electronic transaction is the question of trust as it relates to the transaction itself. To say that an electronic transaction complies with the legal requirements is one thing; to have a sufficient degree of trust in the transaction is something else. What does trusting the transaction mean? When vital business transactions depend on computer and network availability, the parties need to know that these will work properly, without interruption. When remote communications replace personal contacts, the parties need to verify each other's identity. When easily copied and altered electronic records replace signed paper documents, the parties need assurance that records are authentic and unaltered. And when sensitive data is stored electronically, the parties need assurance that the data is protected and accessible. Ensuring that the ceremony of reaching an agreement is sound requires the consideration of four issues: Integrity, Confidentiality, Authentication and Non-Repudiation (ICAN).

Integrity refers to the accuracy and completeness of the communication. Electronic documents are easily altered in a manner that is not detectable. Moreover, because every copy of an electronic document is a perfect reproduction, unlike paper documents, there is no such thing as an "original" electronic document, and electronic records come with no inherent attributes of integrity.

This concern about the "legality" of electronic signatures has persisted not only because of a few court decisions, but also, because of a lack of specific legislative authorization.

The recipient of an electronic message must be confident of a communication's integrity before the recipient relies and acts on the message. A signature can be used to verify the integrity of a document, but clicking a mouse or typing one's name on an easily altered electronic document is no guarantee of document integrity. Typically, the use of cryptographic algorithms, often coupled with digital signatures, is the only way to detect alteration in an electronic document.

The primary concern in confidentiality is unauthorized disclosure: protecting information so that unauthorized persons cannot access it, and, if unauthorized access is obtained, to ensure the information is unreadable (encrypted). Confidentiality may not be an issue in every situation, but it may be necessary to protect attorney-client communications, or obligations arising as a result of contractual commitments. It may also be important for preventing access to and use of information that can cause harm to the owner of the information, such as social security, credit card, or bank account numbers.

Authentication is concerned with the source or origin of a document or message.[28] Is it genuine or a forgery? A party entering a transaction in reliance on an electronic message must be confident as to the source, and must also be able to establish the integrity of its electronic signatures if a dispute occurs. A signature can be used to authenticate the source of a document. In today's digital age, where conversations originate through e-mails, a valid and legal approach to verification can be through the control of an e-mail address coupled with a transaction history that shows a dialog of events.

Non-repudiation stems from authentication and integrity: the ability to prove that the originator of a document in an electronic transaction intended to hold the sender to his communication in the event of a dispute.[29] A person's willingness to rely on an electronic communication, contract or funds transfer request is typically contingent upon having some level of comfort that he can prevent the sender from denying that he sent the communication (if, in fact, he did send it), or from claiming that the contents of the communication as received were not the same as what was sent (if, in fact, they were what was sent). Leveraging a third-party provider to produce consistent results from the sender, as well as the recipient, helps ensure this is not an issue.

Ensuring trust in an electronic transaction requires a secure, consistent process—specifically, the use of security procedures designed to ensure integrity, confidentiality, authentication and non-repudiation of electronic documents and messages. There are a number of security protocols that can be used to assist in establishing trust for electronic communications. These include: repeat-back acknowledgements, date/time stamping, replies and acknowledgments with logs of devices used, algorithms or codes, digital signatures, identifying words or numbers (an e-mail address), using trusted third parties to retain copies of electronic communications, encryption, or using an automated process or system.[30]

Conclusion

Like traditional signatures of ink on paper, electronic signatures come in vary-

ing degrees of security. A handwritten signature is trusted more than a stamped one, and a notarized signature is trusted more than all other forms of signature. As the pressures to become more efficient and "greener" increase, the choice to record electronic signatures is not a question of "if" but "when." Strong multifactor authentication certainly improves security: what is less clear is what end-users will accept as a convenient and usable process. Reflecting the real-world difficulties security managers have, the vendor landscape is complex. There are a variety of electronic signature solutions that help companies achieve a legal electronic signature, but often, companies overlook the portability of legal documents. While some services require users to type-in codes to validate documents, others offer the documents digitally signed in a portable PDF format. Often, the real question is the flexibility and integration features of the system, as most comply with E-SIGN and UETA requirements. The third-party electronic signature service that offers a better means of capturing intent and electronic signatures will make the process easy for end-users and will likely be a successful implementation for your office.

The easiest route is to leverage a third-party electronic signature service provider such as YesDocs, the company I founded. Using YesDocs ensures you will comply with the E-SIGN and UETA laws without the headache of the implementation: all documents are transferrable to your systems in an automated or semi-automated fashion, so you won't ever be without a copy or the supporting audit trail information. Regardless of which solution you leverage, make sure it fits your needs.

Legal disputes are unfortunate but a reality for most governments. Missing or incomplete documentation puts organizations at risk. A reliable set of business records strengthens an organization's legal position when these disputes arise. Be sure to apply the appropriate amount of security in light of the risk. Use professional implementers that are accredited in what they do. Ensure the legal department has the appropriate authority in IT developments that affect the legality of an electronic signature process.

Notes

1. The term "electronic record" is defined as a "record created, generated, sent, communicated, received, or stored by electronic means." *See* Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C. § 7006(4); Uniform Electronic Transaction Act (UETA) at §2(7).
2. The term "data message" is defined as "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." UNCITRAL Model Law on Electronic Signatures, Art. 2(c).
3. "Record" is typically defined as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." *See* E-SIGN, 15 U.S.C. § 7006; UETA at §2(13).
4. "Electronic signature" means "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. E-SIGN, 15 U.S.C. § 7006 (5); UETA, § 2(8).
5. This article will not focus on these aspects; rather, it will review some of the specific requirements for enforceability that might be imposed solely because of the electronic nature of the transaction.
6. FED.R.EVID. 1002.
7. For the Statute of Frauds and contracts involving the sale of goods, *see* U.C.C. § 2-201(1) (1998); *see also* U.C.C. § 1-206 (1998) (limited enforcement of unsigned, unwritten contracts for the sale of securities for $5,000 or more). *See* RESTATEMENT (SECOND) OF CONTRACTS § 110 statutory note, at 284-85 (1982) for a state-by-state listing of state statutes of frauds. Thousands of federal, state, and local laws require certain types of transactions to be documented in writing with a signature. *See* Report of the National Conference of Commissioners on Uniform State Laws (NCCUSL), Uniform Electronic Transactions Act, Task Force on State Law Exclusions (Sept. 21, 1998) at www.webcom.com/legaled/ETAForum/docs/report4.html.
8. *See, e.g.,* Department of Transp. v. Norris, 474 S.E.2d 216 (Ga. Ct. App. 1996), *rev'd sub nom.*, Norris v. Georgia Dept of Transp., 486 S.E.2d 826 (1997) (holding that a fax transmission was not a writing).
9. In the European Union, the enforceability of electronic transactions is governed by the Electronic Signatures Directive adopted in 1999 and the Electronic Commerce Directive adopted in 2000. Globally, the United Nations Commission on International Trade Law (UNCITRAL) Working Group on Electronic Commerce has been developing the laws on the enforceability of electronic transactions, and finalized and approved its Model Law on Electronic Signatures in 2001. *See* the Baker & McKenzie Global E-Commerce Law website at www.bakernet.com/ecommerce for a regularly-updated summary of e-commerce legislation.
10. 15 U.S.C. § 7001 *et. seq.* (West 2010).
11. Each state adopting the law has done so with specific exclusions, resulting in different variations. Illinois, Washington and New York have not adopted the UETA, but have adopted similar laws for electronic signing. A copy of UETA is available at www.law.upenn.edu/bll/ulc/fnact 99/1990s/ueta99.htm. E-SIGN preempts all inconsistent state legislationother than state enactments of UETA in the form promulgated by NCCUSL.
12. For a list of the states that have enacted UETA, *see* The National Conference of State Legislatures at http://www.ncsl.org/IssuesResearch/ TelecommunicationsInformationTechnology/UniformElectronicTransactionsActs/tabid/13484/Default.aspx
13. E-SIGN defines "transaction" as "an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct: (A) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) services, and (iii) any combination thereof; and (B) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof." 15 U.S.C. § 7006(13). UETA defines "transaction" as "an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or

continued on page 36

The City of Bell

cont'd. from page 9

retirement accounts, may have exceeded $1.5 million.
7. For the *Los Angeles Times* reporter's account, see James Spencer, *The Story of How the Bell Scandal Broke: An Account From LA Times Reporter Jeff Gottlieb*, August 11, 2010, *available at* http://www.publicceo.com.
8. Jeff Gottlieb and Ruben Vives, *supra* note 1.
9. Police Chief Randy Adams, who was receiving a salary of over $450,000, was not charged.
10. Richard Winton, *Attorney general's lawsuit against bell officials could be in jeopardy*, L.A. TIMES, November 5, 2010, *available at* http://www.latimes.com
11. Letter from John Chiang, California State Controller, to Pedro Carrillo, Interim City Administrator, City of Bell, dated Sept. 22, 2010, enclosing the report of the State Controller's Office audit. The letter is available online at http://www.sco.ca.gov/Press-Releases/2010/controller_chiang_2010_bell_audit_letter.pdf.
12. Jeff Gottlieb and Ruben Vives, *Benefits push Bell ex-manager's compensation to more than $1.5 million*, L.A. TIMES, August 8, 2010, *available at* http://www.latimes.com.
13. Paloma Esquivel and Robert J. Lopez, *Times investigation: Bell demanded extra fees from some businesses*, L.A. TIMES, November 2, 2010, *available at* www.latimes.com.
14. Ruben Vives and Richard Winton, *Bell generates big money from towing cars; resident demands investigation*, L.A. TIMES, August 2, 2010, *available at* www.latimes.com.
15. Paul Pringle, *Did Steve Cooley's office neglect Bell probe?* L.A. TIMES, October 28, 2010, *available at* http://www.latimes.com.
16. Steve Lopez, *The bleeding Bell blues*, L.A. TIMES, July 21, 2010, *available at* http://www.latimes.com.
17. Paul Pringle, Corina Knoll and Kim Murphy, *Rizzo's horse had come in*, L.A. TIMES, August 22, 2010, *available at* http://www.latimes.com.
18. The survey may be accessed online at http://www.cacities.org/compensationsurvey.
19. The Institute for Local Government has resources on public engagement and collaborative governance on their website at http://www.ca-ilg.org.
20. For examples of social media policies that California cities have adopted, go to http://www.cacities.org/socialmediaresources. ML

Federal

cont'd from page 18

7. Fed. Trade Comm'n, *FTC Extended Enforcement Policy: Identify Theft Red Flags Rule*, 16 CFR 681.1 (Apr. 30, 2009).
8. Brief for Plaintiff-Appellee, *American Bar Ass'n v. Fed. Trade Comm'n*, No. 10-5057 (Aug. 20, 2010).
9. Red Flag Clarification Act of 2010, Pub. L. No. 111-319 (Dec. 18, 2010).
10. *Id.* ML

Supreme Court

cont'd. from page 23

public nuisance against the owners and operators based on their contributions to global warming. (The City alleged that unrestrained emissions of greenhouse gases would increase the temperature in the City, which would, in turn, increase heat-related deaths, damage the coastal infrastructure, and wreak havoc in its residents' daily lives).

The power companies petitioned for a writ of certiorari, challenging the plaintiffs' standing to bring the actions, the existence of a cause of action to cap carbon dioxide emissions under the federal common law, and the existence of justiciable claims. The questions presented in the case are: (1) Whether states and private parties may seek emissions caps on utilities for their alleged contribution to global climate change; (2) whether a cause of action to cap carbon dioxide emissions can be implied under federal common law; and (3) whether claims seeking to cap carbon dioxide emissions based on a court's weighing of the potential risks of climate change against the socio-economic utility of defendants' conduct would be governed by "judicially discoverable and manageable standards," or could be resolved without "initial policy determination[s] of a kind clearly for nonjudicial discretion." See *American Electric Power Co. v. Connecticut*, 582 F.3d 309 (2d Cir. 2009), *cert. granted*, 2010 WL 4922905 (U.S. December 06, 2010) (No. 10-174). ML

Electronic Signatures

cont'd. from page 27

governmental affairs." UETA § 2(16).
14. 15 U.S.C. § 7001(a); UETA § 7.
15. *See* Thomas J. Smedinghoff and Ruth Hill Bro, *Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce*, 17 J. MARSHALL J. COMPUTER & INFORMATION L. 723 (Spring 1999).
16. 15 U.S.C. § 7001(a).
17. UETA §7(a), (c), and (d).
18. *See* E-SIGN, 15 U.S.C. § 7003, and UETA § 3(b) for a complete list of exceptions.
19. 15 U.S.C. § 7001.
20. *Id.* at § 7002(a).
21. UETA § 5(b).
22. *Id.* and comment 3. Some state enactments of UETA (e.g., California) require such consent to be in electronic form.
23. 15 U.S.C. § 7006(5); UETA, § 2(8) (definitions of "electronic signature").
24. 15 U.S.C. § 7001(a) and 7006(5); UETA, § 2(8) and 7(d).
25. For more on Information Assurance, see http://en.wikipedia.org/wiki/Information_assurance.
26. 15 U.S.C. § 7001(e).
27. UETA § 8(c).
28. *See* FED. R. EVID. 901(a) (1995).
29. *See* Information Security Committee, Electronic Commerce Division, ABA Section of Science & Technology Law, *Digital Signature Guidelines* (Aug. 1996), available at www.abanet.org/scitech/ec/isc/dsgfree.html. One definition of non-repudiation is "[s]trong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents." *Id.* at § 1.20.
30. *See* FED. R. EVID. 901(b)(9)(1995). ML