To agree or not to agree: Legal issues in online contracting

Carl Pacini
Assistant Professor of Accounting, Florida Gulf Coast University, Fort Myers

Christine Andrews
Assistant Professor of Accounting, Florida Gulf Coast University, Fort Myers

William Hillison
Arthur Andersen Professor of Accounting, Florida State University, Tallahassee

E-commerce for merchants and consumers is more than just establishing or visiting an attractive Web site to conduct business over the Internet. For companies and consumers alike, conducting business in cyberspace entails not only the traditional risks of sales and contracting, but also a new set of risks related to the electronic environment. For entities of all sizes, important components of those risks involve legal issues: jurisdiction, contract formation, contract validity, contract changes and errors, authentication and attribution, message integrity, and non-repudiation. Becoming familiar with these issues can help avoid costly disputes in e-business.

Companies have been doing business electronically for a number of years. Take electronic data interchange, for example. Defined as the electronic exchange of information between trading partners, EDI has been used successfully by General Electric, General Motors, Sears, Wal-Mart, and a number of other major corporations. Human intervention is often nonexistent, with goods being ordered and delivered and payments initiated via electronic fund transfers (EFTs). Unlike e-commerce transactions, EDI traditionally requires trading partners to use a dedicated leased transmission line or a connection to a value-added network (VAN). Moreover, it involves both a direct connection and high start-up and operating costs—entry barriers that the Internet has lowered through its use of a common information and communication platform.

Or consider Financial Electronic Data Interchange (FEDI), which integrates EFT and EDI and results in both remittance data and fund transfers being accomplished simultaneously. If the seller's bank is not EDI-capable, a buyer can implement FEDI by contracting with a financial value-added network (FVAN), a separate organization that enables the linking of various EDI networks.

However, in nearly all these electronic relationships, prior agreements (called "trading partner agreements") provide answers to most of the legal questions that might arise. Virtually every contingency can be anticipated, and the partners can agree on how to proceed, even over a dispute. In contrast, when e-commerce participants are dealing with strangers over an open system like the Internet, bilateral agreements are harder to arrange. Agreements that anticipate all contingencies cannot be expected to be agreed to by thousands of customers who might visit an e-merchant's Web site.

As the world of e-commerce continues to expand, uncertainty about the enforceability of electronic agreements and the legitimacy of the parties involved has led many executives, attorneys, business owners, regulators, and others to ponder what might happen when disputes arise over electronic transactions. A 1997 court ruling by a

Georgia appellate court has contributed to this uncertainty. In *Georgia Dept. of Transportation v. Norris*, the court held that filing a notice by fax did not satisfy a requirement that notice be in writing because the transmission of "beeps and chirps" along a telephone line is not writing in the customary sense of the term.

The risks or uncertainties related to conducting business over the Internet are:

- *Jurisdiction*—Who has legal jurisdiction over a cybercontract, given the global nature of e-business?
- *Contract formation*—Is a business or other Web site owner making a contractual offer or an invitation to bargain?
- *Contract validity*—What is the legal validity of a Web wrap or click-on contract?
- *Contract changes and errors*—What is the legal effect of changes and errors in transmission over the Internet?
- *Authentication and attribution*—How can parties to a contract be assured that those they are dealing with are legitimate?
- *Message integrity*—Is the message received exactly the same as the message sent?
- *Nonrepudiation*—How can a business or consumer be assured that parties cannot deny the content of a transaction or event?

Given the importance of understanding these various risks, e-business participants should become familiar with the basic legal issues involved. Here we will analyze the status of contract law applicable to e-transactions, provide an overview of recent legislative efforts that have been undertaken to classify e-business contract law, and offer practical suggestions for contracting in cyberspace. It is important to note here that we do not offer legal advice in this article; readers needing legal advice should seek such services from competent legal counsel.

Jurisdiction

Contracting in cyberspace presents a challenge to Web site owners because the Internet is a form of communication that rises above spatial boundaries. Its domain flows indiscriminately across international boundaries as easily as it flows across the street. This creates jurisdiction problems in disputes between e-commerce buyers and sellers, such as where a contract was formed or which state's law applies. Moreover, because Internet technology allows "pull" relationships (a customer reads or downloads information from an e-merchant's Web site) as well as "push" relationships (an e-merchant sends information to a customer automatically), the question of the location of legal contact becomes complex.

In the United States, two different groups of court decisions have emerged with regard to Web sites. One line of judicial authority has granted jurisdiction over nonresidents on the grounds that their Internet involvement encompassed significant interactivity (or follow-on contracts). In *CompuServe Inc. v. Patterson* (1996), a federal appeals court ruled that a computer programmer in Texas was subject to Ohio law. The programmer and Ohio-based CompuServe had formed an electronic contract under which CompuServe distributed and sold copies of software. During contract negotiations, the programmer had never visited Ohio. In *Cody v. Ward* (1997), a federal district court asserted jurisdiction based on telephone and e-mail communications that consummated a business relationship started over Prodigy's "Money Talk" discussion forum for financial matters.

In both these cases, the Internet activities of those subjected to the jurisdiction of a distant court involved more than a visit to a passive Web site. In other cases, reports Takach (1999), courts have asserted jurisdiction based on solicitation of donations, signing up subscribers for Net services, and negotiations and other dealings that occurred as the result of an initial Internet communication.

In a second group of cases, US courts are refusing to exercise jurisdiction over an out-of-state person or business because of mere Web site access or creation. In *Bensusan Restaurant Corp. v. Richard King* (1997), a Missouri jazz club called the Blue Note established a Web site on which it advertised. People wishing to visit the establishment had to telephone to order tickets and physically take delivery of them at the club in Missouri. The Web site also contained a disclaimer that the Blue Note was not affiliated with the famous New York jazz club of the same name. When the New York club brought a trademark infringement suit, the federal court dismissed the action for lack of jurisdiction, reasoning that a Web site that merely provides information is not equivalent to advertising, selling, or promoting in New York City. The federal appeals court deemed it significant that almost 100 percent of the customers of the Blue Note lived in Missouri.

In the 1998 case *IDS Life Insurance Co. v. SunAmerica, Inc.*, plaintiff IDS Life sued SunAmerica for unfair competition, tortious interference with contract, misappropriation of trade secrets, and intentional interference with business relationships. IDS claimed that SunAmerica was inducing IDS's sales agents to leave the company and switch their customers over to SunAmerica in violation of IDS employment contracts. The federal district court refused to find jurisdiction solely on the basis of SunAmerica's operation of a Web site. This case reflects the common approach in the second group of cases in that mere, general Web site access is insufficient to confer jurisdiction on a court over a nonresident defendant.

These two lines of US court decisions suggest the use of a sliding-scale standard in deciding e-business jurisdiction issues that relates to the amount and level of online commercial activity. A clear statement of this standard appears in *Zippo Mfg. Co. v. Zippo Dot Com, Inc.* (1997):

> The likelihood that personal jurisdiction can be constitutionally exercised is directly proportional to the nature and quality of commercial activity that an entity conducts over the Internet....If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmissions of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site that is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.

Figure 1 illustrates the approach taken by US courts in determining jurisdiction issues in commercial cyberspace transactions.

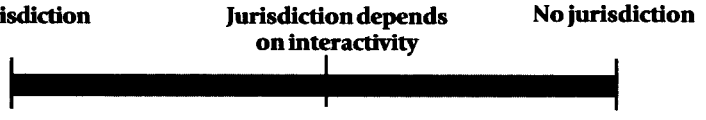
The legal uncertainty faced by e-merchants is increased by dealing with parties from other nations. Conceivably, a foreign court could deem it reasonable to exercise jurisdiction over a US merchant who engaged in an e-business transaction with one of its citizens. Under current law, a foreign nation can usually assert jurisdiction over nonresidents when the exercise of that jurisdiction is "reasonable." According to the American Law Institute (1987), circumstances that have been found to be reasonable include those in which a nonresident was:

- regularly conducting business in a foreign country;
- engaging in an activity outside the foreign country that has a substantial, direct, and foreseeable effect in that country; or
- engaging in an activity that is the subject of court action being owned, possessed, or used in the foreign country.

Businesses that host Web sites can implement measures to reduce the likelihood of being summoned into court in an undesirable jurisdiction. First, the site should include both a forum selection clause (in which state or country a case will be heard) and a choice of law provision (which state's or nation's law applies) that are agreed to when a purchaser decides to buy. In *Burger King v. Rudzewicz* (1985), the US Supreme Court held that forum selection clauses are generally enforceable because a person can consent to personal jurisdiction. However, courts decide their enforceability on a case-by-case basis. On the other hand, in *The Bremen v. Zapata Off-Shore Co.* (1972), the Supreme Court indicated that forum selection clauses must be fair and reasonable to be enforced. These same principles also apply to a choice of law provision.

Caspi v. Microsoft Network (1999) can serve as a useful illustration of these principles. Microsoft Network, an online computer service, required prospective subscribers to view multiple computer screens of information, including a membership agreement containing a forum selection clause. The membership agreement appeared on the screen in a scrollable window next to blocks providing the choices "I Agree" and "I Don't Agree," either of which prospective members had the option to click at any point. A New Jersey appellate court struck down a challenge to the forum selection clause because there was no basis to conclude that it was proffered unfairly or designed to conceal its provisions. The court concluded the plaintiffs knew they were entering into a contract.

Figure 1
Sliding scale standard of jurisdiction in e-commerce cases



Interactive Web site:	*Mixed Web site:*	*Passive Web site:*
• Provides information for users to make purchase decisions • Actively solicits business	• Provides information • Users can exchange information with host computer	• Provides only information • Does not solicit business

Source: Ferrera et al. (2001)

Hence, a brilliantly worded provision on jurisdiction and/or choice of law is not useful unless the Web site owner has brought it to the attention of the user. For example, a forum selection and/or choice of law clause may be unenforceable if it appears only at the foot of the home page and does not appear on subsequent pages. Some Internet users will not visit a Web site via a home page but may do so from a hyperlinked site or from a bookmark list. To help reduce the noted risks, a required checkbox for indicating agreement to a forum selection and/or choice of law clause can be included, placed just before or as part of a transaction execution selection.

Second, the Web site owner should use technology that counts site "hits" (and possibly have it audited by a CPA firm) to document the number of sales in another state or foreign nation. Such evidence could be valuable in demonstrating that the Web site does little or no business in the location where a plaintiff files a lawsuit. Failure to satisfy the "minimum contacts" requirement of due process can result in the plaintiff being unable to establish jurisdiction.

Third, e-business Web site owners should use written disclaimers, which give owners more control over the parties with whom they do business. A site disclaimer clause may state that certain transactions will not be entered into with residents of specific states, provinces, or countries. Moreover, the clause could be used in conjunction with a technology filter that precludes the site from being accessed by visitors from certain states or countries. In the final analysis, those who employ the Net to do business out of state and/or abroad must closely examine the parameters of dealing in cyberspace.

Contract formation

The advent of e-commerce over the Net has raised various legal issues about the formation of electronic contracts. One area of uncertainty is whether a business Web site owner is making an offer or merely an invitation to make an offer. Does the potential customer's communication constitute an offer or an acceptance? The answer will dictate the time and place a contract is made. The question of offer or acceptance was aptly demonstrated recently when an e-merchant in the UK advertised televisions on its Web site for £3.99 instead of £399 because of a computer error. More than 20,000 orders were placed before the e-merchant realized why the televisions were so popular and closed down its site. The legal issue to be resolved is whether displaying goods or services on a Web site amounts to an offer by the seller, which e-consumers accept, or an invitation to negotiate, to which they respond with an offer.

Given the risks, businesses would be well advised to construct a Web site that is, in effect, a "shop window" or an invitation to make an offer. This allows the customer to make an offer to buy goods or services that the site owner is free to accept or reject. The prudent e-business should clearly set out an agreed-upon method of contract acceptance. First, the screen should state in large, bold print that any indication of interest sent by an e-customer is an offer, not an acceptance. Once the e-business receives an offer from a purchaser, it can decide whether or not to accept. It then sends an e-mail to the customer after considering and approving the purchaser's offer. These procedures give greater control to the e-merchant in choosing the terms that will govern the contract.

Contract validity

Another emerging issue is the legal validity of Web wrap or click-on contracts. Such a contract is typically found on a Web site offering goods or services for sale. The e-consumer or e-business wanting to create a legal relationship (buyer and seller) with a Web merchant finds legal terms on the computer screen, often in a dialogue box that permits messages and responses. The consumer usually consents to the terms by clicking a box on the screen that says "OK" or "I agree." The question arises, however, as to when an acceptance occurs in such a situation.

Traditional contract law usually holds that an acceptance is effective when sent by the offeree using an authorized mode of communication. This "mailbox rule" applies unless the offer provides otherwise, the offeree uses an unauthorized method of acceptance, or the acceptance is sent after the offeree sends a rejection. In *Bickmore v. Bickmore* (1996), a Canadian court held that a faxed acceptance of a faxed offer was delivered when the acceptance was sent. The mailbox rule developed, however, in the nineteenth century when contracts were often negotiated at a distance through the mails and the courts had to protect the offeree from losses incurred by any delay or failure on the part of the post office. Given the advent of instantaneous communication, such as the Net, some courts have held that the rationale behind the mailbox rule does not apply. In *Entores v. Miles Far East Corporation* (1955) and *Brinkibon v. Stahag* (1983), two English courts ruled that acceptance is effective upon receipt in situations involving instantaneous forms of communication.

The issue is whether displaying goods or services on a Web site amounts to an offer by the seller, which e-consumers accept, or an invitation to negotiate, to which they respond with an offer.

Thus, if the Net can be regarded as an instantaneous communication medium, then it appears more appropriate to consider that acceptance occurs (or the contract is formed) when the response—the "clicking on an icon"—is received. This principle is a clear abrogation of the mailbox rule, but is consistent with the policy in virtually all EDI model trading partner agreements that have addressed the issue. It is

also consistent with existing or proposed legislation such as the United Nations Convention on Contracts for the International Sale of Goods (CISG), proposed revisions to Article 2 and 2A of the Uniform Commercial Code, the United Nations Model Law on Electronic Commerce, and the Uniform Computer Information Transactions Act (UCITA). "Receipt" does not require that the recipient of the electronic message know of, open, or read the message. All it requires is that the electronic message be available for processing by the recipient's information system.

Contract changes and errors

With recent advances in information technology, the use of software to send or answer messages automatically has moved from the realm of science fiction to business reality. The new technology, referred to as "electronic agents" or "intelligent agents," makes it possible for computers to initiate and complete a transaction without human intervention. In fact, the entire point of the new technology is to allow such transactions to take place without any need for human traders to review or even be aware of particular transactions.

How the law responds to such innovation will have an enormous impact on the development and growth of e-commerce. For example, where no prior EDI agreement exists between the parties, may one of them make an offer or acceptance by machine? Who is responsible if the computer "makes a deal" contrary to the programmer's intention? These questions relate to risk that must be considered by those involved with computer-to-computer transactions.

Currently, the common law is more or less unclear on the legal effect of using an electronic agent even though the policy of "owner responsibility" seems generally accepted. Moreover, two model statutes provide some guidance to those who operate Web sites with electronic agent characteristics. For example, the Uniform Electronic Transactions Act (UETA), which has been adopted by several states, does address the limited circumstance in which a contract is formed solely by electronic agents in an automated transaction. Although UETA applies only to parties who have agreed to conduct transactions by electronic means, it makes clear that a contract may be formed by the interactions of the electronic agents of the parties, even if no individual was aware of or reviewed the agent's actions or the final contract terms. Both UETA and the UN Model Law on Electronic Commerce consider information systems to be instruments of the owner for purposes of forming contracts. Machines or computers may not appear to have the necessary intent required to form a contract, but those who place them in operation for that purpose do have that intent.

Another area of concern in e-commerce is the legal effect of changes and errors in transmission. The common law remains unclear in this area, but UETA offers a practical solution. When a business or person (Party A) conducts an electronic transaction with the Web site of Party B, and if Party B does not allow Party A a chance to correct or prevent an error, the error can be avoided provided that Party A:

- promptly notifies Party B of the error and the fact that Party A did not intend to be bound by the electronic message sent;
- takes reasonable steps, including those that conform to Party B's reasonable instructions, to destroy or to return to Party B (according to Party B's instructions) any item of value received as a result of the erroneous electronic message; and
- has not used or received any benefit or value from the consideration received from Party B.

This avoidance rule is limited to human error when dealing with a machine or computer system.

Resort to the law can be avoided if Party B constructs a Web site that enables an e-customer or e-merchant to prevent the transmission of an erroneous record, or enables an e-customer or e-merchant to correct an error once sent. For example, an electronic agent may be programmed to provide a "confirmation screen" to the e-customer with the ability to prevent the erroneous record from being transmitted. Similarly, the electronic agent might receive the transmission sent by the e-consumer and then send back a confirmation that the person must accept before the transaction is consummated. In either case, the electronic agent would provide an opportunity to prevent or correct any error.

Authentication, attribution, and nonrepudiation of electronic contracts

Another key issue in e-commerce is the problem of attributing an electronic message to the person who purports to send it. Although cyberspace involves anonymity, e-customers and e-merchants must be matched up with legally responsible parties in the real world. Those involved in e-business must confront issues linked to the authentication of an electronic message sender. First, consumers and businesses want to know that they can rely on a message as having actually been sent by the purported sender. Second, e-commerce participants wish to avoid liability in the event a message allegedly sent by one party was actually sent by an interloper or hacker.

Both UETA and UCITA take the position that an electronic record (information that is inscribed on a tangible medium or stored in an electronic or other medium and is retrievable in perceptible form) or signature (a mark made with the intention of authenticating the marked document) is attributable to a person or entity if it was the act of the person or entity. One's actions include those of both human and electronic agents. For example, an electronic signature on a purchase order, in response to a declining inventory level, is attributable to a person whether it originated with that person, an employee, or a software program (intelligent or electronic agent).

UETA and UCITA also indicate that the person's act may be attributable in virtually any manner. This includes any security procedure used to determine the person or entity to which an electronic record or signature can be attributed. A "security procedure" is one employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person, or for detecting changes or errors in the information in an electronic record. The term includes procedures that require the use of algorithms or other codes, passwords, encryption, or callback, or any other acknowledgment procedure. Security procedures are, in fact, only one way of attributing an electronic communication to a specific party or entity.

According to UCITA, a receiving party, acting in good faith, who properly applies an attribution procedure and ascertains that a message was from a given party can bind that party. An electronic communication may be attributed to a party when:

- the message was dispatched by one who obtained the necessary access number or device(s) from a source under the control of the alleged sender;
- the access occurred because of the purported sender's failure to exercise reasonable care in protecting the number or device; and
- the receiving party relied upon the message to his, her, or its detriment.

In essence, one who negligently permits an electronic message to be sent is bound by that communication to anyone who detrimentally relies on it.

Electronic signatures

A common attribution procedure used in the e-business environment is an electronic signature. Traditionally, a signature is any mark or symbol affixed to a writing to manifest the signer's intent to adopt it as his own and to be bound by it. UETA defines an electronic signature as an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. Numerous types of electronic signatures have been developed through advances in technology. However, the two primary categories are: (1) non-cryptographic methods and (2) cryptographic methods. The former are designed primarily to mitigate identification and authentication risks. The latter provide controls necessary to meet the additional risks of nonrepudiation and security. The spectrum of electronic signature technologies currently available is discussed below.

Non-cryptographic controls

Password or personal ID number. Passwords and PINs have been used as controls over access to information for many years to authenticate a user and allow access to a computer network. However, it should be recognized that the role of a PIN or password is just that of authentication. In other words, the user who has the PIN provides a form of assurance that he is the authorized person. In this sense, the PIN is a form of electronic signature. To function properly, it must be known by both parties prior to use. Use of the PIN over an open communication channel can create additional problems. It is usually essential that the PIN be encrypted so that it cannot be intercepted and learned by others.

Smart card. A smart card contains an embedded chip that can generate, store, and/or process data. The card can be used to facilitate various authentication technologies when inserted into a reader device. Information from the card's chip is read by security software only when the user enters a PIN or password or provides a biometric identifier. This method provides greater security than use of a PIN alone because a user must have both (1) physical possession of the smart card and (2) knowledge of the PIN. This type of control is common with ATM transactions. Because of the physical nature of the card (or any other physical form of identity), it is termed a "token." Good security requires that the smart card and the PIN be kept or stored separately.

Digitized signature. A digitized signature is a graphical image of a handwritten signature recorded by digital pen and pad. By using special software, the recipient compares the digitized representation of the entered signature with a stored copy of the graphical image of it. A digitized signature is more reliable for authentication than a PIN because there is a biometric component to the creation of the handwritten image. In other words, the recording device and associated evaluation software compare not only the shape of the letters but also the timing of each pen stroke, its duration, and/or the pen pressure. Forging a digitized signature can be more difficult than on paper because digital comparisons with a computer program are more discriminatory than those done with the human eye.

At first glance, this form of electronic signature appears to be well suited for authentication. It is not only difficult to forge, it also maintains a format familiar to manual approaches. However, the user-created image on the digital pad is literally a stored digital file to be compared to the maintained version. If the digital signature file is sent

electronically, it is subject to interception, copying, and later resubmission by parties other than the signer. Thus, just like PINs, digitized signatures should not be sent over open networks unless encrypted.

Biometrics. Individuals have unique physical characteristics that can be converted into digital format to be recorded in a file and interpreted by a computer. Among these are voice patterns, fingerprints, and patterns present on the retina of one or both eyes. In this technology, the physical characteristic is measured by a microphone, optical reader, or some other device, converted into digital code, and then compared with an authenticated copy of that characteristic stored in the computer. No matter the type of biometric measure, the resulting code is stored in a file. If the security file is compromised, impersonation becomes a serious risk. Thus, again, such information should be sent over open networks only when it is encrypted.

Cryptographic controls

Symmetric encryption. In symmetric encryption, both the sender and receiver have access to the same key, which is not known publicly. If Paul wants to send Sally an encrypted message, he uses a key to encode the message and transmits the message to Sally. Sally uses the same key—and only that key—to decrypt the message. Because the same key performs these two functions, and only Paul and Sally know it, Sally knows the message must have come from Paul. This form of encryption provides assurance about authentication as well as privacy and nonrepudiation. Keeping the key secret, however, is paramount and difficult to manage with multiple users.

Forging a digitized signature can be more difficult than on paper because digital comparisons with a computer program are more discriminatory than those done with the human eye.

The most popular and widely used private-key cipher is the Data Encryption Standard (DES), the federal standard enunciated in 1977. Today, a more secure variant of DES, called Triple DES (because it applies the encryption algorithm three times using different keys) is now widely used in the private sector. Other alternatives to DES have been developed by RSA Data Security, including RC2, RC4, and RC5. DES, however, is soon to be replaced by a new federal standard.

In October 2000, after a three-year global competition, the US Department of Commerce announced that an encryption algorithm named Rijndael is the proposed new Advanced Encryption Standard (AES). Reavis (2001) reports that security products should be available by early 2002, based on AES. Rijndael will be unclassified, free of any royalties, and publicly available for use and export anywhere in the world.

Asymmetric encryption. Two researchers at Stanford University developed public key cryptography because of the difficulties involved in exchanging and managing private keys. Unlike symmetric key cryptography, this asymmetric encryption uses an algorithm with a public key and a private key that are mathematically linked. The private key is kept secret by the owner while the public key is freely available. One key can only decrypt a message encrypted with the other key. Given this unique characteristic, the two-key set can be used in creating electronic signatures. The first one can be a signing key that is kept private, while the second one can be used as a public validation key that is available to all other parties. Thus, if Paul encrypts a message with his private key that can be decrypted by Sally with Paul's public key, Paul must have sent it because he is the only one with a key who can encrypt a message that can be decrypted by the public key. As long as the private signing key is kept privy only to Paul, the integrity of the process can be virtually assured. And as long as the receiving party can gain access to the public key, the authenticity objective can be met. As with symmetric key encryption, the length of the key dictates the strength of the protection offered by symmetric encryption. Thus, given a key of sufficient length, public key cryptography can provide protection similar to that of private key techniques.

Although the public key method is highly effective, several operational shortcomings must be overcome. The first entails recognizing that just because a public key decrypts a message does not ensure that it is the key of the person it is intended to represent. Anyone could make a key public and claim it to be that of another party. Current practice makes the public key part of a "digital certificate" (or digital signature), a specialized electronic document provided by a trusted party called a Certificate Authority. The CA investigates the identity of the party and maintains a protected record of his public key. A receiving party who receives a signed message from a purported person obtains the public key from the CA as part of the digital certificate. Again, if the message can be decrypted using the certified public key, then the receiver can be confident that it is from the assumed party.

The second shortcoming of public key encryption is its inefficiency. Whereas symmetric keys are typically short—perhaps 40 or 128 bits—asymmetric key technology

requires the keys to be long, typically 1,024 bits. This creates considerable overhead in encryption and decryption that makes sending and receiving long messages impractical. One method used to mitigate this problem is to create a "hash" from the original message and then just encrypt the hash as a signature.

Hashing refers to the process of creating a short string of characters, also called a "digest," from the original plaintext message. After creating a message digest, the sender's private key encrypts it and it becomes a digital signature. The recipient uses the sender's public key to decrypt the message digest and confirm the identity of the sender. Digital signatures ensure not only the authenticity of the sender but also provide for nonrepudiation by binding the sender of a message to its contents. However, it should be noted that because the public key is available to anyone, the message, though encrypted by the sender's private key, is not secure. It could be intercepted and read by anyone having the sender's public key prior to receipt by the intended recipient.

The third shortcoming relates to extending the use of this technology to meet security risk. The most popular technology now in use to secure retail e-business is Secure Sockets Layer (SSL). For example, someone logging on to a Web site can order flowers or books by clicking an appropriate selection and entering a credit card number. SSL is the security protocol that encrypts the order and credit card information to provide secure e-commerce, using a combination of private and public key encryption. In lay terms, the computers of the two parties use public key encryption techniques for authentication purposes and generate, encode, and send a secret private (symmetric) key to be used in sending the actual messages. This is the "best of all possible worlds"; authentication can take place, the message can be communicated securely and efficiently, and nonrepudiation risks can be mitigated.

Legal status of e-signatures

E-SIGN, the Electronic Signatures in Global and National Commerce Act, took effect on October 1, 2000, allowing electronic signatures or documents to satisfy most existing legal requirements for written signatures, disclosures, or records. Its implementation, however, does not mean that all e-signatures and records are now automatically legally binding. It does mean that for any transactions involving interstate or global commerce, any laws or regulations that require the use of signatures or written documents cannot be used to deny the validity or legality of the transaction merely because electronic records and signatures were used. The most important exception for e-business is that E-SIGN does not affect the laws governing contracts or business transactions but is an overlay on those laws. If a signature must be notarized or made under oath, then a certifying official using an e-signature can satisfy the requirement.

The new law makes several notable exceptions for certain contracts and other records that must still be completed in writing and accompanied by a standard manual signature. This list includes wills, codicils, testamentary trusts, cancellation notices involving health and life insurance (other than annuities), legal documents related to family law (such as divorce decrees), court orders and notices, and default notices and foreclosure documents related to a person's primary residence. E-SIGN also does not affect the writing requirement attached to records and documents governed by the Uniform Commercial Code, such as checks, drafts, certificates of deposit, notes, letters of credit, bulk transfers, warehouse receipts, and security interests in personal property. The new law also does not affect the rights of holders of most securities against securities issuers. In general, it allows e-signatures or documents to satisfy most existing legal requirements for written signatures. On the other hand, it neither entirely eliminates risks related to e-signatures and documents nor ensures their enforceability. Nor does it require any person to agree to use electronic signatures.

E-SIGN sets forth certain conditions for the enforcement of electronic transactions. Where an existing law mandates that a contract be in writing, such as the Statute of Frauds,

Figure 2
Pointers for contracting in cyberspace

1. A Web merchant should state which court has jurisdiction as part of the contract terms before entering into e-commerce transactions. Careful consideration should be given to the degree of interactivity incorporated into a Web site; toll-free numbers subject the e-merchant to the jurisdiction of a court in the state in which the e-customer resides.
2. An e-merchant should construct a Web site as a shop window, allowing the customer to make an offer to buy goods or services. The e-merchant can then accept or reject the offer.
3. In business-to-business (B2B) e-commerce, where both parties have agreed to conduct business by electronic means, electronic agents may form contracts because those who placed them in operation had the intent to contract.
4. Confirmation screens should be used to give consumers an opportunity to prevent the transmission of erroneous orders and correct an error once sent.
5. Security procedures should be used so e-consumers and merchants can be matched with legally responsible parties.

the enforceability of the electronic record of the contract requires that record to be capable of being retained and "accurately reproduced" for later reference. Another condition of enforcement is that any action taken electronically must be attributable to the person to be bound.

E-SIGN is "technology-neutral," anticipating the use of electrical, digital, magnetic, wireless, optical, and electromagnetic means for e-signatures. It also contains various consumer protection provisions. First, a consumer must have "affirmatively consented" to the use of electronic communication, and must not have withdrawn such consent. Before consenting, the consumer must receive certain disclosures. In a "clear and conspicuous" statement, the consumer must be informed of:

- the right to have a record of the transaction provided on paper;
- the right to withdraw the consent to have the record provided in electronic form;
- the fact that any consent provided applies only to a specific transaction;
- how to obtain a copy of any electronic message sent and whether any fee will be charged for a copy;
- the procedures required to withdraw any consent provided; and
- the type of hardware and software needed to access and retain any electronic record created by the transaction involved.

The law is written in such a fashion as to not restrict or impinge on preceded consumer protection laws.

As e-commerce grows, Web site owners remain concerned about the outcome of potential disputes or lawsuits over many aspects of online contracting. E-businesses can increase the likelihood of avoiding a costly dispute by gaining a basic familiarity with the legal issues involved (see **Figure 2**).

To establish jurisdiction, business Web sites should be constructed to include both a forum selection clause and a choice of law provision, both of which should be part of the contract terms. E-commerce participants should consider what actions by buyers and sellers lead to forming a contract, and the prudent Web site owner should set forth an explicit means of contract formation (offer and acceptance). Because the use of electronic agents creates uncertainty in contract formation—May one make an offer or acceptance by machine?—a Web site should enable e-commerce participants to prevent the transmission of an erroneous record or to correct one after transmission. When it comes to electronic messages, e-consumers and e-merchants alike must be matched up with legally responsible parties in the real world. Both must know that they can rely on a message as having actually been sent by the purported sender, and avoid liability in the event a message was sent or altered by an interloper or hacker. Finally, e-commerce participants must know the laws regarding e-signatures, PINs, smart cards, digitized signatures, biometrics, and various forms of encryption. Because E-SIGN now allows electronic signatures to satisfy most existing legal requirements for written signatures, documents, or records, laws or regulations that require the use of signatures or written documents cannot be used to deny the validity of the transaction merely because electronic signatures and records were used. This is true for any transactions involving interstate or global commerce. ❍

References and selected bibliography

American Law Institute. 1987. *Restatement (Third) of the Foreign Relations Law of the United States* §421. New York: American Law Institute.

Beattie, C.R. 2000. Facilitating electronic commerce—The Uniform Electronic Transactions Act. *Uniform Commercial Code Law Journal* 32 (Winter): 243-269.

Bensusan Restaurant Corp. v. Richard King. 1997. 126 F.3d 25 (2d Cir.).

Bernstein, L., and G. Kaplan. 2000. The Electronic Signatures Act: Giving a boost to e-commerce. *ABA Bank Compliance* (September): 21-26.

Bickmore v. Bickmore. 1996. 7 C.P.C. (4th) 294 (Ont. Ct.(Gen. Div.)).

Boss, Amelia, and J.K. Winn. 1997. The emerging law of electronic commerce. *The Business Lawyer* 52 (August): 1,469-1,502.

The Bremen v. Zapata Off-Shore Co. 1972. 407 U.S. 1.

Brinkibon v. Stahag Stahl and Stahlwarenhandelsgesellschaft m.b.H. 1983. 2 A.C. 34 (H.L.).

Burger King v. Rudzewicz. 1985. 471 U.S. 462.

Caspi v. Microsoft Network, LLC. 1999. 732 A.2d 528 (N.J. Super. Ct. App. Div.).

Cody v. Ward. 1997. 954 F.Supp. 43 (D. Conn.).

CompuServe Incorporated v. Patterson. 1996. 89 F.3d 1257 (6th Cir.).

Entores v. Miles Far East Corporation. 1955. 2 Q.B. 327 (C.A.).

Ferrera, G., S. Lichtenstein, M. Reder, R. August, and W. Schiano. 2001. *CyberLaw.* Cincinnati: Thomson Learning.

Georgia Dept. of Transportation v. Norris. 1997. 474 S.E.2d 216 (Ga. App. 1996), *rev'd on other grounds,* 486 S.E.2d 826 (Ga.).

Gregory, J. 1999. Solving legal issues in electronic commerce. *Canadian Business Law Journal* 32 (July): 84-131.

Harrison, A. 2000. Feds propose new encryption standard. *Computerworld* (9 October): 14.

IDS Life Insurance Co. v. SunAmerica Inc. 1998. 958 F.Supp. 1268 (N.D. Ill. 1997), *aff'd in part, vac. in part,* 136 F.3d 537 (7th Cir.).

Kerr, I. 1999. Spirits in the material world: Intelligent agents as intermediaries in electronic commerce. *The Dalhousie Law Journal* 22 (Fall): 190-249.

Lui-Kwan, K.M. 1999. Recent developments in digital signature legislation and electronic commerce. *Berkeley Technology Law Journal* 14 (Fall): 463-481.

McIntyre, J.T. 2000. The electronic signature law and its impact on financial planners. *Journal of Financial Planning* (September): 36-38.

Miller, Roger, and F. Cross. 2002. *The legal and e-commerce environment today.* 3rd ed. Cincinnati: Thomson Learning.

Moss, V. 2000. Congress enacts new e-signature law. *Credit Union Magazine* (September): 87-89.

Oliveira, L., P. Amorim, and C. Vilao. 1999. Electronic commerce. *International Financial Law Review* (January): 39-43.

Pinsky, L. 2000. Digital signatures: A sign of the times. @ www.lsus.edu/classes/csc101/spring98/mar24/gorydetl.htm (October).

Reavis, J. 2001. Goodbye DES, hello AES. *Network World* (July): 1-3.

Takach, G. 1999. Internet law: Dynamics, themes and skill sets. *Canadian Business Law Journal* 32 (July): 1-83.

Winn, J.K., and M.R. Pullen. 1999. Despatches from the front: Recent skirmishes along the frontiers of electronic commerce. *The Business Lawyer* 55 (November): 455-496.

Zippo Mfg. Co. v. Zippo Dot Com, Inc. 1997. 952 F.Supp. 1119 (W.D. Pa.).