Online Contracts

G. E. Evans, *Queen Mary Intellectual Property Research Institute, UK*

INTRODUCTION

The global organization of networked computers that we call the Internet has given contracts a new role and dimension. Contracts have become the very building blocks of electronic commerce. Not only do they perform an essential function as the purveyors of software and content licenses, but they also provide the core infrastructure for the exchange of informational products in networked markets. In fact, one of the five key principles of the *A Framework for Global Electronic Commerce* (White House, 1997) relies on the establishment of a legal environment based on a contractual model of law. In a renaissance of freedom of contract, licensors are charged with the freedom to order contractual relationships as they see fit to market their products online and, in so doing, advance the growth of the new economy. One of the clearest indications of the new economic trajectory may be seen in the significant returns of the software sector. The actual and estimated return of the combined hardware, software, and services sectors was $536.8 billion for the U.S. economy during 2003 (U.S. Department of Commerce, 2003).

Since the idea of open-architecture networking was first introduced in 1972, the Internet has revolutionized the communications world in an unparalleled manner. Whether we are talking about selling intangible or tangible goods, the Internet has dramatically changed not only business–customer relations but also the way in which products are distributed and exchanged. Computer networks make possible new vertical and horizontal business relationships between producers, users, consumers (P2P), and suppliers (B2B). In response, Internet business models, whether virtual or clicks-and-mortar, are assuming an increasing variety of forms, including the following: brokerage, advertising, informediary, merchant, manufacturer, affiliate, community, subscription, and utility (Afuah & Tucci, 2000). Moreover, the supply of goods and services directly between supplier and consumer has given rise in turn to new classes of business intermediaries. From the business communities of aggregators to the online auctions, all rely on contracts to provide stable online trading markets, a trading venue defined by clear rules, industrywide pricing, and open market information for buyers. eBay.com, for example, was among the first successful sites to provide a framework where consumers could trade a wide variety of goods and services with each other (consumer-to-consumer, C2C) and with business (consumer-to-business, C2B).

Arguably, we might think of shrink-, click-, or browsewrap agreements as a new kind of *lex mercatoria*

P1: pdb
JWBS001B-97.tex WL041/Bidgoli WL041-Bidgoli.cls November 10, 2005 10:51 Char Count= 0

or merchant-designed law to facilitate the online exchange of goods and services in consumer markets. In contrast to traditional contracts, there is a far greater degree of uncertainty as to online contracts' validity and enforceability, particularly in the areas of jurisdiction, contract formation, identification of the terms and statutory issues relating to signature, and other evidentiary requirements. For example, vendors and merchants question how an offer should be made and acceptance given. Buyers are concerned that one false click might result in their being ensnared into entering a binding contract.

Through a combination of mercantile custom, common law, and legislative developments, the classic principles of contract law are being adapted and supplemented to accommodate the needs of electronic commerce. The aim of this chapter is to provide the reader with an overview of the law relating to the formation and validity of electronic contracts and to offer some recommendations concerning the measures that might be taken to create an enforceable electronic contract. The first part of this chapter describes the problems pertaining to contracting online, including the maintenance of security of electronic transactions and the integrity of electronic documents. The next part considers the legal framework for electronic contracting, notably with respect to the provision of standards and procedures for electronic signature. The next section examines the enforceability of clickwrap and browsewrap licenses that the software industry has pioneered to facilitate online transactions of its products and to give additional security to its intellectual property. In a medium where it is all too easy to include unduly harsh terms, this section also discusses the doctrine of unconscionability, which may subsequently render a contract unenforceable, and how to guard against such a contingency. The chapter then discusses the vexed question of contractual restrictions in end user license agreements, including limitations on the fair use of software, the means of dispute resolution, and the forum in which licensees can bring suit. The next section examines the problems that have arisen with respect to the licensing of digital information and sales law, particularly warranties concerning the fitness and merchantability of informational goods, such as software. The chapter then considers the developments that have taken place with respect to consumer rights online, in particular the ability of consumers to enjoy the legal protection offered by their home states. The chapter concludes with some tips and suggestions for contractors as to how, given the current state of the law, they might best offset the risks of contracting online. Although this chapter generally deals with contractual issues associated with the security of online commerce, other security-related considerations that also affect the validity of online contracts are beyond its scope and are covered in other parts of this handbook: network security (Volume I, Part 2: Infrastructure for the Internet, Computer Networks and Secure Information Transfer), protocol standards (Volume I, Part 3: Standards and Protocols for Secure Information Transfer), and security management (Volume II, Part 3: Foundations of Information, Computer, and Network Security).

MAINTAINING THE SECURITY OF ELECTRONIC TRANSACTIONS

Problems Concerning the Authenticity and Integrity of Electronic Documents

Authenticity is concerned with the source or origin of a document or message ([Fed. R. Evid. 901]). Integrity is concerned with the accuracy and completeness of the communication. In a paper-based world, a contracting party can rely on numerous indicators of trust to ensure the authenticity and integrity of a document. These indicators include using paper, perhaps with a letterhead or watermarks, or other indicia of trust, to which the message is attached and not easily altered; handwritten ink signatures; sealed envelopes for delivery via a trusted third party, such as the postal service or a courier service; or personal interaction between the parties. However, with electronic documents and electronic communications conducted remotely over the Internet, none of these indicia of trust is possible. To all intents, a communication in binary code can be copied and modified easily without discovery. In addition, although a handwritten signature can be readily verified to authenticate the identity of the signer and the source of a document, online there is an additional risk that the party contracting may not be who they claim or that the substance of the communications used to form an agreement may be subject to alteration.

Party Authentication and Message Integrity

Moving transactions to an electronic environment has two important consequences. First, in many cases it may be difficult to know when one can rely on the authenticity and integrity of an electronic message. Authentication issues, although rare in the real world, become increasingly important in the virtual world (see the chapter in this handbook, Anonymity and Identity on the Internet). On the Internet, how do we decide whether Jane Doe is who she says she is? Those decisions that involve entering into contracts, shipping products, making payments, or otherwise incurring financial risk are difficult to make when relying on an electronic message. Second, in the event of legal action, this lack of reliability can make it extremely difficult to prove the validity of the contract in court. For example as an evidentiary matter, if the defendant denies making the "signature" that is attached to an electronic document, it may be impossible for the plaintiff to prove the authenticity of that electronic signature, in the absence of additional evidence (e.g., *U.S. v. Eisenberg,* 1986; *U.S. v. Grande,* 1980).

The concern regarding integrity arises from the fact that electronic documents are easily altered in a manner that is not detectable. Further, because every copy of an electronic document is a perfect reproduction, the original of an electronic document does not exist. How then are we to know whether the document the recipient received is the same as the document that the sender sent? How do we know whether the document has been altered either in transmission or storage?

If users are to have trust in the electronic medium, recipients of electronic messages must be confident of

the communication's accuracy (Smedinghoff, 2002). The question of integrity is critical when it comes to the negotiation and formation of contracts online, the licensing of digital content, the making of electronic payments, and the verification of the authenticity of these transactions at a later date. For example, a contractor who wants to receive tenders from bidders online must be able to verify that the messages containing the bids have not been altered. In that situation, the use of cryptographic algorithms, accompanied by digital signatures, is the best means of detecting any alteration in an electronic document.

If the commercial world is to benefit from the advantages of online contracts, both buyers and sellers need to be assured that online contracts are secure insofar as the identity of the parties and the certainty of the terms are concerned. The Statute of Frauds, which requires that certain contracts, such as those dealing with transfers of land, be in writing, was designed to overcome the problem of fraud with respect to oral contracts. Although the principle is still a sound one, to condition the enforceability of an online contract on a requirement for pen-and-paper writing would present a barrier to the effective use of the electronic medium (Prefatory Note to the Uniform Electronic Transactions Act, 7a, Part I, U.L.A. 17 (supp. 2000)).

THE LEGAL FRAMEWORK FOR ELECTRONIC CONTRACTING

United Nations Model Law on Electronic Commerce

With a view to removing barriers to electronic transactions, the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce of 1996:

- establishes rules and norms that validate and recognize contracts formed through electronic means
- sets default rules for contract formation and governance of electronic contract performance
- defines the characteristics of a valid electronic writing and an original document
- provides for the acceptability of electronic signatures for legal and commercial purposes
- supports the admission of computer evidence in courts and arbitration proceedings

U.S. Laws Covering Electronic Transactions

These principles were implemented in the United States in 1999, when the National Council of Commissioners on Uniform State Laws (NCCUSL) approved the Uniform Electronic Transactions Act (UETA), 7A, Part I, U.L.A. 17 (Supp. 2000), which facilitates the use of electronic documents and electronic signatures. As of June 2004, 46 states have enacted the UETA (see http://www.ncsl.org/). In addition, the Uniform Computer Information Transactions Act (UCITA), also approved by NCCUSL in 1999, among its substantive provisions on electronic contracts, includes articles validating electronic transactions for the "licensing" of computer data (National Conference of Commissioners on Uniform State Laws, 2001b). Concerned at the slowness and lack of consistency with which UETA was being adopted by state legislatures, in 2000 Congress stepped in to enact the Electronic Signatures in Global and National Commerce Act (E-SIGN; Pub. L. No. 106–229, 114 Stat. 464 (2000)).

Finally, Article 2 of the Uniform Commercial Code (UCC), which has governed the sale of goods since its promulgation in 1951, has recently been amended to accommodate electronic commerce and to reflect the development of business practices, changes in other law, and interpretive difficulties of practical significance (National Conference of Commissioners on Uniform State Laws, 2002). Adopted on May 13, 2003 by the NCCUSL and the American Law Institute (ALI), the amended Article 2, section 2-108(4) is intended to modify, limit, and supercede E-SIGN. In addition to the potential difficulties of application concerning its interface with E-SIGN, amended Article 2 (Sales) is not a revolution in sales law. The provisions of amended Article 2 include substitution of the word "record" for "writing" throughout amended UCC Article 2 and the adoption of new language concerning contract formation in amended UCC 2-204, 2-211, 2-212, and 2-213. In states that do not adopt amendments to UCC Article 2, E-SIGN (or UETA to the extent that it preempts E-SIGN) will apply to transactions subject to Article 2. In states that do adopt amended UCC Article 2, E-SIGN will not govern transactions subject to Article 2.

Formation and Validation of Electronic Contracts

As a matter of general principle, there is no requirement that the parties to a contract must indicate their consent to be bound by signature. In fact, the law provides that a contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties that recognizes the existence of such a contract (UCC § 2-204). Similarly, E-SIGN provides that "a contract . . . may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation" (§ 101(a)(2)). In addition, UETA provides that "a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation" (§ 7(b)). Finally, the UNCITRAL Model Law on Electronic Commerce is even more explicit in providing that "an offer and the acceptance of an offer may be expressed by means of data messages" and "where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose" (Article 11(1)).

As a general rule, offers to contract may be made orally, in writing, or by conduct. There is no reason in principle therefore why an offer that is electronically transmitted should be any less effective than a written one. The problem is largely one of evidence. Questions may arise concerning the reliability of electronic communications, which may make it more difficult to introduce evidence in court. To be valid, an offer must communicate to the person receiving it that, once the offer is accepted, a contract is created. An offer may be accepted "in any manner and

P1: pdb
JWBS001B-97.tex WL041/Bidgoli WL041-Bidgoli.cls November 10, 2005 10:51 Char Count= 0

by any medium reasonable in the circumstances" (UCC 2-206(1)(a)). Online offers may be accepted by e-mail or other form of electronic message, by electronic agent, and by conduct, such as clicking on a button or downloading content. Thus, if an offer is made by e-mail, one should be able to accept it by the same means unless the offer states otherwise (Restatement (Second) of Contracts § 65).

Although, generally speaking, an acceptance does not necessarily have to be sent the same way as the offer (*Market Development Corp. v. Flame-Glo Ltd.,* 1990), UETA provides that an electronic record is considered received only when it enters a computer system "that the recipient has designated or uses for the purpose of receiving electronic records of the type sent" (§15(b)(1)). Consequently, if the parties have regularly corresponded in the past by e-mail, an e-mail acceptance sent to the offerer's e-mail address will presumably be effective. The purpose of the UETA requirement is to assure that recipients can designate the e-mail address or system to be used in a particular transaction in the event the parties have multiple e-mail addresses.

When Is an Electronic Record Sent or Received?

Issues surrounding the timing of electronic records may be essential for resolving questions as to whether a binding contract has been created, as in the case where the offeror sets a deadline for acceptance. In addition, electronic transmissions may pose similar problems to cases where the offer and acceptance were exchanged by fax or other means of communication in which the interaction is not immediate. In the case where a message is sent from one computer system to another, UETA provides that the time at which an electronic record is considered to have been sent is the time that the record "enters an information processing system outside the control of the sender"; in the case where a message is sent from one person to another on the same system, such as where both parties are using the same Internet service provider, it is the time that the record "enters a region of the information processing system designated or used by the recipient which is under the control of the recipient" (§ 15(3)). An electronic record is considered to have been sent as of that time, provided that it is addressed properly to an information-processing system that the recipient has designated or uses for the purpose of receiving electronic records and from which the recipient is able to retrieve the electronic record, and provided further that it is in a form capable of being processed by that system (UETA § 15(a)(1) and 15(a)(2)).

Conversely, UETA provides that an electronic record is considered received by the intended recipient when it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records of the type sent and from which the recipient is able to retrieve the electronic record, and is in a form capable of being processed by that system (§ 15(b)). It is also important to note that an electronic record is considered received even if no individual is aware of its receipt. That is, as with the postal service, once the message is delivered, it makes no difference whether the addressee actually opens it.

Automated Transactions

Can a computer be said to have entered into a contract? Generally speaking, it may do so, depending on the circumstances. Certainly, a computer is capable of generating an offer. Inventory systems for example, are designed to calculate when supplies are low and automatically generate an electronic purchase order to the vendor. By analogy, case law indicates the validity of such contracts (*State Farm Mutual Auto. Ins. Co v. Bockhorst,* 1972). The law accepts that the computer operates in accordance with the information and directions supplied by its programmers. Similarly, a computer-generated acceptance, as distinct from a mere acknowledgment of receipt, may serve to create a binding contract (*Corinthian Pharmaceutical Systems v. Lederle Labs,* 1989). Accordingly, an electronic data interchange (EDI) message, such as a purchase order acknowledgment, would be considered an appropriate acceptance.

With respect to the related question of the enforceability of contracts formed via electronic agents, both E-SIGN and UETA expressly recognize the validity of such contracts. An electronic agent is defined as a computer program or other automated means used to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response (E-SIGN § 106(3); UETA § (2)(6)).

E-SIGN provides that a contract or other record relating to a transaction may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound (§ 101(h)). Similarly, UETA recognizes that a contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agent's actions or the resulting terms and agreements (§ 14(1)). In addition, UETA recognizes that a contract may be formed by the interaction of an electronic agent and an individual (§ 14(2)). Likewise, UCITA provides for the making of contracts bymeans of an "electronic agent" (s.102) and provides for the validation of electronic contracts to the extent that it validates contracts made by "electronic agents" or preprogrammed computer programs (ss. 107 and 206).

Notice and Consent Requirements

Because electronic contracts involve additional risks when compared with traditional transactions, both E-SIGN and UETA expressly require that the parties agree to enter into their transaction electronically before it will be considered enforceable. Conversely, as there is no obligation on the parties to do so, they are entitled to refuse to enter into the transaction in electronic form (E-SIGN, 15 U.S.C. § 7001(b)(2); UETA §s 5(a)). As to the question whether the parties have "agreed to conduct transactions by electronic means" (UETA § 5(b); E-SIGN, 15 U.S.C. § 7001 (c)), their agreement may be either express or implied and is to be objectively determined from the surrounding circumstances, including the parties' conduct (UETA § 5(b)). Although some state enactments of

UETA—for example, that of California—require such consent to be in electronic form in order to provide greater certainty, in other states consent may be implied from conduct. For example, in the event one party launches a Web site that is capable of entering into electronic transactions and the other party accesses that Web site and proceeds to enter into an electronic contract with the first party, there is a strong inference that the parties have implicitly agreed to conduct business electronically.

E-SIGN's Consumer Consent Provisions

Whereas the provisions of UETA concerning consent to transact electronically apply equally to commercial and consumer transactions, E-SIGN contains special requirements for businesses that want to use electronic records or signatures in consumer transactions. It requires businesses to obtain from consumers electronic consent or confirmation to receive information electronically that is required by law to be in writing. This would be the case for example, with laws requiring written disclosure of interest rate charges in consumer loan transactions. The act went into effect in October 2000 (15 U.S.C. § 7001(c)). Section 101(c)(1) of the act provides that information required by law to be in writing can be made available electronically to a consumer only if he or she affirmatively consents to receive the information electronically and the business clearly and conspicuously discloses specified information to the consumer before obtaining his or her consent. Moreover, Section 101(c)(1)(C)(ii) states that a consumer's consent to receive electronic records is valid only if the consumer "consents electronically or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent." Presumably, the obligation to "reasonably demonstrate" ability to access the information may be met if the consumer merely states in an electronic message that he or she can access the electronic records in the specified formats or otherwise acknowledges or responds affirmatively to an electronic query that asks whether the consumer can access the electronic record (Federal Trade Commission, 2001; Consumer Consent Provision in Section 101(C)(1)(c)(ii)).

Signature Requirements

The requirement that the parties sign their transaction has three purposes: (1) the signature serves as an expression of intent, (2) it may be required by law, and (3) it may be necessary for the security of the transaction. With respect to the first purpose, a signature provides *prima facie* evidence of the signer's intent with respect to the document signed. Of course, the nature of the signer's intent varies with the transaction and in most cases can be determined only by looking at the surrounding circumstances in which the signature was made. For example, a signature may indicate an intent to be bound to the terms of a contract, the approval of a request by an employee or person designate for funding of a project, authorization to a bank to transfer funds, or simply that the contents of a document have been made known and that the other party has had an opportunity for review.

Concerning the second purpose, a signature is often the means employed to satisfy a law that requires the fact of signature before the document will be considered legally binding. The Statute of Frauds is probably the best known of the numerous federal and state statutes that require certain types of transactions, such as the sale of land or contracts for the sale of goods in excess of the stipulated monetary limit (Amended Article 2 (Sales), 2002, increases the threshold amount to $5,000), to be documented in writing and to be signed. In this regard, the increasing weight that courts tend to be placing on e-mail communications and electronic signatures should put buyers on their guard. Prospective buyers should ask themselves whether they are willing to be contractually bound by offers that are made by e-mail, because the e-mail sender's act of typing his or her name at the bottom of the e-mail may be sufficient to manifest intention to authenticate the transmission for Statute of Frauds purposes. The copy of the e-mail in question submitted as evidence of an intention to contract has been held sufficient for the purpose. In the case of *Rosenfeld v. Zerneck* (2004), for example, the plaintiffs had e-mailed the defendant, confirming their offer to purchase the defendant's home for $3.5 million. The defendant accepted the offer via e-mail. The typed signature at the bottom of the defendant's e-mail was held to satisfy the requirement that a "writing be subscribed under New York State's general Statute of Frauds" (General Obligations Law § 5-701), for the New York legislature had amended that provision to allow for the subscription of electronically transmitted memoranda.

Finally, a signature often functions as a means of security, in the sense that it can be used either to authenticate a document, notably for the purposes of identifying the source of the document, or to ensure the integrity of the document to the extent that it has not been altered by an unauthorized source. It is for this reason, for example, that parties to a multipage contract sometimes initial each page of the contract. In the electronic environment, certain types of signatures (e.g., cryptographically created digital signatures) can play an important role in verifying the integrity of the entire document.

Definition of Electronic Signature

Traditionally, the law has allowed any symbol (e.g., the notorious "x"), that is made with the intent to sign a document to qualify as a legally valid signature. Hence, the definition of "signed" in the Uniform Commercial Code includes "any symbol" as long as it is "executed or adopted by a party with present intention to authenticate a writing" (Article 1, § 1-201(39) (1999)). The law is chiefly concerned with the signer's "intention to authenticate" the document by affixing her signature and thereby indicating her intention to be legally bound.

Both E-SIGN and UETA extend the traditional approach of the law to the concept of an electronic signature. To be enforceable, they require that an electronic signature meet the following three criteria (E-SIGN, 15 U.S.C. § 7006(5) and UETA § 2(8)):

1. be a sound, symbol, or process.
2. be attached to or logically associated with an electronic record. This requires that the parties implement

an electronic recordkeeping process that is capable of providing evidence that a specific signature was applied to or used in connection with a specific document. The easiest way to comply with this requirement is to have the signature incorporated as part of the electronic record that is stored.

3. be made with the intent to sign the electronic record to the end that the signature relates to a specific document and to evidence the signer's intent with respect to that document.

The European Union (EU) Electronic Signature Directive uses a similar definition of an electronic signature. Under the directive, an electronic signature must also meet three criteria: (1) be data in electronic form, (2) be attached to or logically associated with other electronic data, and (3) serve as a method of authentication (Electronic Signature Directive, Article 2(1) AA). For the majority of transactions electronic signatures that meet these requirements will be considered legally enforceable as substitutes for handwritten signatures (UETA §s 2(8) and 7(d); E-SIGN, 15 U.S.C. § 7001(a) and 7006(5)).

Methods of "Signing" an Electronic Record

The definition of an electronic signature acknowledges that there are a variety of methods by which an electronic record may be signed. Although an electronic signature, by its nature, must be represented digitally—that is, in binary code—it can take many forms and can be created using a variety of different technologies. Well-known examples of electronic signatures that satisfy E-SIGN and UETA include the following:

- a name typed at the end of an e-mail message by the sender (*Shattuck v. Klotzbach*, 2001)
- a digitized image of a handwritten signature that is attached to an electronic document
- a PIN number that identifies the sender to the recipient
- a unique biometrics-based identifier, such as a fingerprint
- a mouse click as illustrated by the ubiquitous "I accept" button
- a "digital signature" created through the use of public key cryptography

"Digital Signatures" Created by Public Key Cryptography

There is a considerable difference, however, between an electronic signature that merely satisfies the requirements of E-SIGN and UETA and a trusted, certified electronic signature. As we have noted, when transactions are automated and carried out remotely, using digital technology that can easily alter the record, it becomes critical to have a means of ensuring the identity of the parties and the integrity of the document. Merely clicking on an "I accept" button or typing a name on an e-mail message offers no evidence as to the authenticity of the signature.

Because most legally recognized electronic signatures provide only a weak level of authentication, they have to be accompanied by certification procedures. Parties who wish to conduct their business by electronic means would be well advised to use the services of one of the many certification authorities. VeriSign, Baltimore Technologies, RSA Security, and Pretty Good Privacy are some of the companies that offer digital signature technologies and certification services. A digital signature is the sequence of bits that is created by running an electronic message through a one-way hash function to create a unique digest (or "fingerprint') of the message and then using public key encryption to encrypt the resulting message digest with the sender's private key.

Encryption technology through public key infrastructures (PKI) is employed to enhance security. Public key cryptography employs an algorithm using two different but mathematically related cryptographic keys: one for creating a digital signature or transforming data into a seemingly unintelligible form and the other key for verifying a digital signature or returning the message to its original form (American Bar Association Section of Science and Technology Electronic Commerce Division Information Security Committee. Digital Signature Guidelines. August 1, 1996. Available at: http://www.abanet.org/scitech/ec/isc/dsgfree.html.) Such digital signatures allow the sender of a document or a message to encrypt that message or document with a unique, private key. The message recipient is then able to decrypt the document using a related public key.

Most governments have undertaken initiatives to promote the use of digital signature and encryption technology in the public and private sector. In contrast with E-SIGN, the EU Directive for example provides a comprehensive regulatory framework. It envisions the growth of a complex network of competing and complementary PKIs providing electronic certificates to customers that, in turn, can be used by these customers to sign documents electronically.

Record Accessibility Requirements

Another key requirement for the enforceability of electronic transactions is that the documents that comprise the transaction should be communicated in a form that can be retained and reproduced accurately by the receiving party. 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" (15 U.S.C. § 7001(e)). Similarly, 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" (§ 8(c)).

That is not to say that this requirement limits electronic transactions to those parties that possess the technical capability for downloading or printing documents. Rather, the focus is on the form of the document as communicated by the sender and essentially requires that the sender do nothing to inhibit the ability of the recipient to download, store, or print the applicable record. The fact that the recipient may choose to use a device without such capabilities, such as a PDA or other handheld device without a

print capability, should not affect the enforceability of the transaction. On the other hand, such provisions clearly call into question the form of clickwrap agreement typically used on many Web sites in which the agreement is displayed in a separate window from which it cannot be downloaded or printed.

Record Retention Requirements

An essential element for the enforceability of all transactions is record keeping. In the event of a dispute, it is necessary to produce reliable evidence documenting the terms of the transaction and the agreement made by the parties. For electronic transactions, this issue raises questions as to whether the keeping of electronic records is sufficient to satisfy the applicable statutes, regulations, or evidentiary rules and, if so, what requirements must be met for acceptable electronic records. Both E-SIGN and UETA address this issue directly and impose similar requirements. In essence, storage of an electronic record will satisfy legal record retention requirements if the stored copy of the electronic record meets the following two criteria:

1. accurately reflects the information set forth in the record (E-SIGN, 15 U.S.C. § 7001(d)(2); UETA § 12(b))
2. remains accessible for later reference to all persons who are entitled to access by law, for the period required by the relevant statute and in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise (UETA § 12(a); E-SIGN, 15 U.S.C. § 7001(d))

With respect to evidentiary rules, both 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 (E-SIGN 15 U.S.C. § 7001(d)(3); UETA § 12(d)). These provisions also make clear that records can be kept in electronic-only form. Furthermore, they provide considerable flexibility to the parties in terms of how they store the records, when and whether they wish to store the records on new media, and how to meet applicable evidentiary requirements.

ENFORCEABILITY OF ONLINE CONTRACTS

Characterizing Shrink-, Click-, and Browsewrap Agreements

Clickwrap agreements may be seen as analogous to shrinkwrap agreements, the original character and form of which are generally attributed to software producers and their desire to find a satisfactory method of distributing software held on CDs or diskettes and sold in packaged form. Likewise, clickwrap agreements are online contracts that invite users to scroll through their terms and conditions before manifesting their assent to contract by clicking on a button that states "I accept" or "I agree." A third form of online contract that is rapidly gaining favor because of its user friendliness is the browsewrap agreement. In this form of agreement, a notice is simply placed on the Web page informing users that they are subject to a license agreement, which is available for online viewing at any time.

The enforceability of clickwrap and browsewrap agreements and the security of the intellectual property they purport to protect are of critical importance, in view of the fact that such agreements have become the common means of exchange for consumer goods in networked markets worldwide. Although the intention to contract might be signaled by the user's clicking on the "I accept" button, the validity and hence the security of clickwrap agreements are by no means as easily assured. Intention is but one of the essential elements necessary to the formation of a legally binding contract. As a matter of general principle, the law also requires one party, usually the seller, to make an offer setting out the terms of the proposed contract to another party, the buyer. A valid contract is formed when an unequivocal acceptance of the offer is communicated to the offeror or seller.

Manifesting Assent to Clickwrap and Browsewrap Agreements

If a clickwrap or browsewrap agreement is implemented properly, it should operate to create a valid and binding online contract between buyer and seller. Both E-SIGN and UETA explain that the "process" of clicking a mouse can qualify as a signature if the other applicable requirements are also present. As the Reporter's note to UETA explains, "this definition includes as an electronic signature the standard webpage click-through process. For example, when a person orders goods or services through a vendor's web site, the person will be required to provide information as part of a process which will result in receipt of the goods or services. When the customer ultimately gets to the last step and clicks 'I agree,' the person has adopted the process and has done so with the intent to associate the person with all the record of that process" (§ 2, comment 7). More broadly, with respect to the formation of such contracts, the courts are guided by the principles of sales law as contained in Article 2-204 of the UCC (Uniform Commercial Code), which states that "a contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract."

The classic case on the validity of such contracts is *ProCD v. Zeidenberg* (1996), where the Seventh Circuit held that software shrinkwrap license agreements are a valid form of contracting under Wisconsin's version of the Uniform Commercial Code. In ringing affirmation of the recent trend to also uphold clickwrap contracts, the federal district court of Minnesota in *I-Sys Inc. v. Softwares Inc*. (2004) rejected an argument that clickwrap acceptance of a software license under protest did not bind the defendants. According to the terms of the license, installation and use of the software with the license attached constituted acceptance of the 1995 and 1998 license terms. The 1995 and 1998 licenses were shrinkwrap agreements, meaning that a file was installed together with the software containing a license document instructing users that by using the software they were accepting the license terms. Subsequently, in 2001 software updates were distributed by means of a clickwrap license that

P1: pdb
JWBS001B-97.tex WL041/Bidgoli WL041-Bidgoli.cls November 10, 2005 10:51 Char Count= 0

required users to accept the terms by clicking through a series of screens before they could access the software. Plaintiff software developers contended that, by not returning the software with a 1995 or 1998 license and by clicking through the 2001 license, the defendants had accepted the terms of the license and were bound by it. The defendant software distributors argued that they were unaware of the 1995 and 1998 licenses and only "accepted" the 2001 license under protest because they needed the updated software that came with it. The court rejected the defendants' argument that they did not truly "accept" the license terms, but clicked through only because they needed the software to upgrade earlier, unsatisfactory versions. It found that references to the licenses in invoices and in the software development agreements gave the defendants sufficient notice of them.

Until recently, the enforceability of browsewrap agreements, in which the terms and conditions are typically posted on the Web site by way of a hyperlink, had been in some doubt. Courts had generally been reluctant to enforce the terms of an agreement that lacks any formal indication that the user has read and agreed to the terms of the contract (*Pollstar v. Gigmania Ltd.,* 2000; *Ticketmaster Corp. v. Tickets.com, Inc*., 2000). However, in a landmark decision affirming the enforceability of browsewrap licenses, the U.S. Court of Appeal for the Second Circuit found Verio Inc., having accepted the plaintiff's terms of use, to be in breach of contract (*Register.com Inc v Verio Inc*., 2004). Register.com derived its authority to act as a registry for the issuance of domain names from a standard form agreement with the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit corporation established by the U.S. government to administer the domain name system. Under the agreement with ICANN, Register was required to maintain a publicly available 'WHOIS' database of registrants' contact information and was not to impose restrictions on the use of this data, except in relation to mass solicitations by e-mail or spamming. Register established a WHOIS database, which it updated on a daily basis, and provided a free public inquiry service for the information contained therein. Register's responses to WHOIS queries were captioned by a legend stating that by submitting a query, the user agreed not to use the data to conduct mass solicitations of business by e-mail, direct mail, or telephone. Contrary to the terms of use, Verio developed an automated software program or robot to access the WHOIS database and compile substantial lists of new domain name registrants whom Verio then proceeded to bombard with unsolicited marketing by e-mail, direct mail, and telephone. Register demanded that Verio cease the practice, but Verio complied only in part—ceasing the e-mail solicitations but continuing to promote its services by direct mail and telephone.

When Register brought suit for breach of contract, Verio argued that because they had not received adequate notice, they could not be said to have consented to the restrictive terms and were therefore not contractually bound to comply with them. In this case notice of the restrictive conditions did not appear until after Verio had submitted the query and received the WHOIS data. Contrary to the Ticketmaster case, the Court of Appeals found that online contracts do not always require formal acceptance by the offeree. Rejecting the need for a requirement that users click an "I agree" icon, the Court of Appeals drew on the general principles of contract law to find that the terms of use in Register's browsewrap agreement, combined with Verio Inc.'s conduct in repeatedly utilizing the WHOIS database, constituted a valid offer and acceptance, thereby resulting in a legally enforceable contract with Verio. Of course, had Verio's utilization of the database been irregular or occasional, it might not have been deemed to have accepted Register's terms of use. In the event, however, the Court upheld the preliminary injunction enjoining Verio Inc. from either utilizing a search robot to obtain information from the plaintiff's database or utilizing information derived from it for mass solicitation.

The Court of Appeals distinguished the facts in Register.com from its former decision in *Specht v. Netscape Communications* (2002). In that case the question for the court was whether plaintiffs were bound by an arbitration clause in the agreement. The Second Circuit held that under the terms of the license agreement to which plaintiffs agreed, governing their use of Netscape's browser, they were under no obligation to arbitrate the claims they raised in the litigation. The software in question could be downloaded from a page on defendant Netscape's Web site by clicking on a button that said "download." When plaintiffs proceeded to initiate installation of the Communicator, they were automatically shown a scrollable text of that program's license agreement and were not permitted to complete the installation until they had clicked on a "Yes" button to indicate that they accepted all the license terms. However, the terms of the license agreement were not contained on this Web page, and the only notice users received of the license agreement was found on a portion of the Web page below the download button. Typically, this notice appeared "below the fold" and was not on that portion of the page that first appeared on the user's screen when he or she proceeded to download the program. This notice informed users that their use of the software would be governed by the terms of a license agreement, which could be seen by clicking on a link provided on the Web page. Once the program was downloaded, the user received no further notice of either the license agreement or its terms. The Second Circuit Court of Appeals found that the plaintiffs were not bound by the terms of the license agreement because they had neither had reasonable notice of the restrictive terms nor had they adequately manifested their assent to be bound by them.

Notice of Unusual or Onerous Terms

Although the general trend at both the legislative and judicial spheres is, in principle, to endorse the validity of clickwrap contracts, that does not mean that the contract is necessarily enforceable. Case law reveals that problems can arise in two areas in particular: the form of assent and the reasonableness of the contractual terms. The legal problems associated with such agreements concern the conditions for the formation of a valid contract and the identification of contractual terms. A contract's terms and conditions are fixed at the moment the contract is formed. Contractual provisions will form part of the agreement

only if the other party has reasonable notice of them before agreeing to contract.

Reasonable notice for unusual and onerous provisions requires greater time than does reasonable notice for normal provisions. This is a particularly significant issue since the clickwrap license is commonly used to unilaterally set out the sellers' terms to the purchaser. Thus the standard software license tends to include a conspicuous notice of title retention in the seller, restrictions on transfer and modification, prohibition of reverse engineering, limited copying provisions, and a forum selection or arbitration clause.

In *Forest v. Verizon Communications Inc*. (2002), the question was whether a forum selection clause mandating that claims be brought in a particular jurisdiction should be applied to a class action suit involving plaintiffs' attempts to register for and use Verizon's broadband service. The subscribers argued that Verizon had not provided sufficient notice of the forum selection clause or its consequences. To become broadband subscribers, users had to agree to all the terms of the agreement, including the forum selection clause. The clause was found in the final part of the agreement, which was available for viewing in a scroll box; however, the box was only large enough to enable users to view a small portion of the document at any time. Users were on notice to 'read the following agreement carefully." The contract was entered into by the subscriber clicking an "Accept" button below the scroll box. The District of Columbia Court of Appeals found that users were provided with adequate notice of the forum selection clause, stating that "the general rule is that absent fraud or mistake, one who signs a contract is bound by a contract which he has an opportunity to read whether he does so or not." The court noted that in reading through the agreement before it was accepted, users would have inevitably discovered the forum selection clause. Nevertheless, it pointed out that the use of a "scroll box" that displays only part of the agreement at any one time is detrimental to the provision of adequate notice (see also *Caspi v. Microsoft Network,* 1999; *CompuServe, Inc v. Patterson*, 1996; *I Lan Systems v. Netscout Service Level Corp.*, 2002, concerning the incorporation of a clause limiting liability).

Similarly in the earlier case of *Hill v. Gateway 2000, Inc*. (7th Cir. Jan. 6, 1997), the Seventh Circuit Court of Appeals held that the "accept-or-return" agreement was effective, stating "competent adults are bound by such documents, read or unread." Although it is not necessary for the buyer to have read the agreement to be bound by it, clearly failure to read the terms can result in substantial loss. Thus, in *M.A. Mortenson Co., Inc. v. Timberline Software Corp*. (2000), the plaintiff sought recovery of $1.95 million, based on an alleged software malfunction that resulted in a project bid of $1.95 million lower than intended. The court followed the reasoning of *ProCD* and *Hill* to find that Mortenson's use of the software constituted its assent to the agreement, including the license terms.

Contracts Voidable for Unconscionability

The enforceability of contracts generally may be affected by particularly onerous or unconscionable terms in standard consumer contracts. The common law of contract has traditionally been able to provide relief when one party is so clearly incapable of looking after his or her interests; in other words, that to enforce the contract would be unconscionable or against all conscience. This principle is codified in Section 2-302 of the UCC, which provides that where a court finds the contract or any clause of the contract to have been unconscionable at the time it was made the court may refuse to enforce the contract, or it may enforce the remainder of the contract without the unconscionable clause, or it may so limit the application of any unconscionable clause as to avoid any unconscionable result. The courts do not set aside private bargains lightly, and the test of unconscionability is notoriously difficult to satisfy. The terms of an unconscionable transaction must suggest that one party took unfair advantage of the party with the disability. Thus, offering to buy a Picasso drawing at a rock-bottom price from a 92-year-old impecunious widow who is unaware of its true market value would be *prima facie* unconscionable.

Nonetheless, in a medium where it is all too easy to create unrealistically one-sided commercial contracts, drafters of online contracts should bear in mind the doctrine of unconscionability to ensure that particularly onerous or unusual (and potentially "unfair") terms are brought to the attention of the persons with whom they are contracting with or risk a court later determining such contracts to be unenforceable. Moreover, even if incorporated properly into a contract, certain terms, such as unreasonable exclusion clauses or limitations of liability, may nevertheless not be enforced against buyers who agreed to a contract of adhesion or standard form contract.

Almost all unconscionability cases have elements of both procedural and substantive unconscionability. Procedural unconscionability involves the manner and process by which the terms become part of the contract. For example, these practices are unconscionable: the use of incomprehensible or legalistic fine-print standard form contract provisions; binding the buyer to additional written terms after the contract is signed; switching contract documents at the last moment to include non-negotiated, one-sided terms; and pressuring the client to sign a contract before reading it. Substantive unconscionability involves the terms of the contract themselves that are unreasonably, unacceptably, or unfairly harsh and against good conscience. Potentially unconscionable clauses would include those authorizing venue or jurisdiction in distant forums, disclaimer of warranties, and limitations or waiver of remedy clauses.

The following case is illustrative: in Comb v. PayPal, Inc., (ND Cal. 2002), plaintiffs successfully claimed that even if they had concluded the user agreement, this agreement, and in particular its arbitration clause, was unconscionable. The court held that PayPal's user agreement was a contract of adhesion, and hence procedurally unconscionable, because it was a form agreement drawn by PayPal, a party of superior bargaining power, and offered to its customers on a take-it-or-leave-it basis. The court also found that the user agreement and its arbitration provisions were substantively unconscionable. In reaching

P1: pdb
JWBS001B-97.tex WL041/Bidgoli WL041-Bidgoli.cls November 10, 2005 10:51 Char Count= 0

this conclusion, the court pointed to several provisions contained in the agreement, including the following:

- PayPal could amend the agreement at any time without notice to users, and these amendments would be binding on them.
- PayPal could freeze all of the funds in a customer's account pending its resolution of any dispute.
- The arbitration provisions mandated arbitration pursuant to the commercial rules of the American Arbitration Association (AAA), which was cost prohibitive, in light of evidence that such a procedure would cost $5,000, whereas the average PayPal transaction was $55.
- The arbitration provision required all arbitrations to proceed in Santa Clara County, California, where PayPal was headquartered, whereas PayPal's customers resided throughout the United States.
- The arbitration provision prohibited joinder of claims among individuals, requiring each instead to proceed individually.

Taken as a whole, these provisions rendered the user agreement and its arbitration provisions unconscionable. The court accordingly denied PayPal's motion to compel arbitration.

CONTRACTUAL RESTRICTIONS ON THE USE OF SOFTWARE

Copyright Preemption, Fair Use, and Reverse Engineering

It is common practice among software companies to study competitors' products in order to improve their own offerings. In this context, the legality of *reverse engineering*, a procedure that generally involves converting machine code back to source code, was recently called into question after the U.S. Supreme Court denied leave to appeal in *Bowers v. Baystate Technologies Inc*. (2003). The Supreme Court's denial of Baystate's petition tends to implicitly affirm the decision of the Federal Court of Appeals that private parties can indeed contract to prohibit the reverse engineering of their intellectual property. A divided Appeals Court found that the federal Copyright Act does not preempt state contract law that allows parties to impose a ban on reverse engineering.

In this controversial case, Harold Bowers had obtained patent and copyright protection for computer-aided design (CAD) software that he distributed under a shrinkwrap licensing agreement that prohibited reverse engineering. Baystate then developed a competing product, which incorporated features of Bowers' software. Bowers alleged Baystate had not only infringed his copyright but also breached the end use license agreement (EULA) by reverse engineering his software in order to modify its own competing software package. For its part, defendant Baystate claimed that it had only evaluated a competitor's product in order to improve its CAD software and that it had not violated encrypted source code. Moreover, Baystate argued that federal copyright law preempts terms that limit the use of copyrighted materials.

Copyright law permits fair use of the work in the form of clean room reverse engineering. Section 117 of the Copyright Act permits an owner of a computer program to make an adaptation of that program provided that the adaptation is either "created as an essential step in the utilization of the computer program in conjunction with a machine" (§§117(1)) or "is for archival purpose only" (§§117(2)). The Court of Appeals found that federal copyright law does not preempt the terms of the contract and upheld the shrinkwrap license. Its decision of January 2003 upheld the decision of the lower court in awarding the plaintiff US$5.27 million for breach of contract and patent infringement.

Nonetheless, contractual prohibitions on reverse engineering remain controversial (Reichman, 1999). In Bower's case the Appeal Court was split, the dissenting judge finding that with respect to nonnegotiated contracts such as shrinkwrap licenses, the contract claim was indeed preempted by federal copyright law. Judge Anthony Dyk chose to follow the decision of the Fifth Circuit in *Vault Corp. v. Quaid Software Ltd.* (1988). He took the view that restrictions on reverse engineering represented the thin end of the wedge. If today software developers were permitted to eliminate the fair use defense, then tomorrow they could also restrict a purchaser from asserting the "first sale" defense, embodied in 17 U.S.C. §109(a) or any other of the protections Congress has afforded the public in the Copyright Act.

In the case cited, Quaid reverse engineered Vault's program in order to create its own program, called RAMKEY, which disabled PROLOK's copy protection. In the course of writing RAMKEY, Quaid loaded the PROLOK program into its computer memory. The court rejected Vault's claim of copyright infringement. The plaintiff's principal claim was founded in Louisiana law. Quaid breached its license agreement by decompiling or disassembling Vault's program in violation of the Louisiana state licensing law that permits a software producer to impose a number of contractual terms upon software purchasers when the license agreement accompanies the producer's software (La.Rev.Stat.Ann. §§§§51:1963 & 1965). Enforceable terms include the prohibition of (1) any copying of the program for any purpose and (2) modifying and/or adapting the program in any way, including adaptation by reverse engineering, decompilation, or disassembly (La.Rev.Stat.Ann. §§51:1964).

Although the restrictions in Vault's license agreement were consistent with the state statute and *prima facie* enforceable under Louisiana's License Act, the District Court found that it conflicted with several areas of federal copyright law. First, although the License Act authorizes a total prohibition on copying, the Copyright Act allows archival copies and copies made as an essential step in the utilization of a computer program (17 U.S.C. §§117). Second, although the License Act authorizes a perpetual bar against copying, the Copyright Act grants protection against unauthorized copying only for the life of the author plus (then) 50 years (17 U.S.C. §§302(a)). Third, although the License Act places no restrictions on programs that may be protected, under the Copyright Act, only "original works of authorship" can be protected (17 U.S.C. §§102. Vault, 655 F.Supp. at 762-63).

With respect to the questions of the preemption of federal law based on section 301 of the Copyright Act, the Federal Appeals Court found that the provision in Louisiana's License Act, which permits a software producer to prohibit the adaptation of its licensed computer program by decompilation or disassembly, conflicts with the rights of computer program owners under §§117 and clearly "touches upon an area" of federal copyright law. Because Louisiana's License Act "touched upon the area" of federal copyright law, its provisions were pre-empted or superseded by the fair use provisions of the Federal Copyright Act. As a result Vault's efforts to prohibit this activity under Louisiana law was illegal. This finding was consistent with the Supremacy Clause of the U.S. Constitution and its role in precluding any state laws that conflict with expressed federal policy in fields where the federal government exercises substantial control (*Bonito Boats, Inc.v. Thunder Craft Boats, Inc*., 1989; *Kewanee Oil Co. v. Bicron Corp*., 1974).

To allow software vendors unilaterally and without restriction to impose terms that prohibit reverse engineering is inimical to the free flow of ideas and information and would frustrate the policy of encouraging the creation of innovative and interoperable software products. Yet, how can small software developers stay in business if larger companies can simply reverse engineer the product before they have been able to recover their investment? Software vendors and content providers rely on contracts to reinforce their intellectual property rights in the digital environment where the risk of unauthorized reproduction and distribution is so much greater. Bower's company, HLB Technology, epitomized the small to medium-sized enterprise driven out of the market by big business. The defendant had not only incorporated features of Bower's product but, having acquired the company with which Bower's held a distribution agreement, it also proceeded to repudiate the contract.

The problematic state of the relationship between copyright and contract is a reflection of the difficulty the licensor has in monitoring licensee use of software and in distinguishing between licensees likely to breach terms of the license essential to the protection of valuable intellectual property (Nimmer, 1998). In the earlier case of *ProCD* the Court of Appeals for the Seventh Circuit also dealt with the preemption issue as to whether federal copyright law disallowed enforcement of the contractual restrictions on use of informational content. The question for the court in *ProCD* was whether the buyer's promise not to make commercial use of the uncopyrightable data in the plaintiff's directory interfered with the balance drawn in the Copyright Act. Previously in *Feist Publications v. Rural Telephone Service Co*. (1991), the U.S. Supreme Court had ruled that the unoriginal compilation of data, such as white pages listings in telephone directories, was unprotectable by copyright law. The Supreme Court's decision seemed to regard such information, once published, as being in the public domain and therefore able to be appropriated freely. A mass-market license term prohibiting the redistribution of telephone listings was ostensibly contrary to the Supreme Court's ruling.

Hence in *ProCD v. Zeidenberg* the defendant argued that the Copyright Act preempts the enforcement of such contracts. The appellate court, however, disagreed. Judge Easterbrook, writing for the majority, found no problem of preemption once he differentiated between contractual rights that are good against the parties to the agreement only, and property rights that are good against the world. Because there was an "extra element" of agreement, the state contract claim was not "equivalent" to a copyright claim. Hence, federal policy did not preempt enforcement of the contractual restrictions.

The issue remains a live one. The migration of software distribution systems to networked environments poses both new risks and new possibilities of risk management for licensors. To the extent that access controls can be placed on software and brought within the Digital Millennium Copyright Act framework (1998), the large corporate licensors have been successful in gaining new tools for controlling the volume of infringing activities. As a matter of technical self-help, the ability to monitor the use of software is also increasing and provides licensors not only with more information about potentially infringing activities but also with the necessary foundation for new pricing models.

SALE OF GOODS LAW AND DIGITAL INFORMATION TRANSACTIONS

Is a Computer Information Product a "Good" or a "License"?

Case law shows that contracts for the transfer of intangible property test the very limits of established law concerning the sale of goods. As a threshold matter, its application is problematic because the product involved is a transaction of "goods," as defined in UCC Article 2 to mean "all things (including specially manufactured goods) which are movable at the time of identification to the contract for sale." To distinguish between transfers that consist largely of intangible as opposed to tangible property, proposed amendments to the Uniform Commercial Code (UCC) in Article 2, section 2-103 (2003), state that the term "goods" expressly excludes "information." However, neither Revised Article 2 nor Revised Article 1 defines the term "information" (National Conference of Commissioners on Uniform State Laws, 2001a, 2002), The Official Comment to §2-103 declares, "This article does not directly apply to an electronic transfer of information, such as the transaction in *Specht v. Netscape* (2002)."

Revised Article 9 clarifies that software is ordinarily not a good and is a "general intangible" except in some limited cases of embedded software. Consequently, although Article 2 would not apply directly to a download of software or digital content, the sale of "smart goods" such as an automobile would be covered fully by Article 2, even though it incorporates many computer programs. In the case of *Specht*, the Second Circuit Court of Appeals observed that downloadable software "is scarcely a tangible good." It chose instead to base its decision on the common law of contracts of California and the Restatement (Second) of Contracts, as it declined to enforce the terms of a license concerning mandatory arbitration that appeared below the "Download" button on a portion of the

Web page that was not visible on most visitors' screens until they scrolled to the bottom of the page.

Whether and to what extent Revised Article 2 applies to a transaction that includes both goods and information are to be determined from all the facts and circumstances. In effect, the amendments to Article 2 leave the courts to sort out in individual cases the UCC's application to computer and software licensing transactions. Generally speaking, with respect to the question whether an online transaction should be characterized as a "sale" or a "license," courts have been accustomed to looking at the totality of the circumstances of the transaction, including such factors as whether a single copy or multiple copies are transferred, whether the transaction involves the physical movement of goods, how the payment is structured, the duration of the agreement, who retains title to the copy for purposes of loss, and the tax treatment of the transaction (*Applied Info. Mgmt. Co. v. Icart*, 1997). In allowing the common law to develop an appropriate body of principles for informational transactions online, the Uniform Computer Information Transactions Act (UCITA), promulgated expressly with the aim of bringing uniformity and certainty to the rules that apply to software transactions, is likely to play its most influential role to date. In view of the problems that may be associated with characterizing software as goods or services, business and software vendors would be well advised to address this distinction expressly in the terms of the contract.

Warranties as to Fitness and Merchantability

Sales and consumer law traditionally protects the buyer's legitimate expectation that the goods will be of merchantable quality (UCC 2-314: implied warranties of merchantability) and fit for the purpose for which they were bought (UCC 2-315: fitness for a particular known purpose). Additionally, revised Article 2 would considerably expand the risk of liability for breach of the warranty of good title. Current law makes sellers liable if they actually do not have "good title"; Revised Article 2-312 creates liability any time that a third party makes a "colorable claim" to title.

In the information economy, however, the problem the law has to confront is that software vendors and content providers, by typically characterizing the transaction as a license to use the software or content and not a sale as such, thereby purport to preclude the application of the UCC's implied warranties. Should the licensor wish to disclaim all implied warranties in a mass-market license, it is sufficient to state the following: "except for express warranties stated in this contract, if any, this information is being provided with all faults, and the entire risk as to satisfactory quality, performance, accuracy, and effort is with the user, or words of similar import." In addition, under current law licensors appear to have the advantage where computer viruses are concerned—that is, destructive computer instructions designed to damage or destroy intangibles—insofar as the principal basis for liability is a warranty of merchantability, which is routinely disclaimed in both negotiated and mass-market licenses. Thus, in *Specht* for example, the terms of the communicator license agreement included a complete disclaimer of warranties ("as is"), an entire-risk clause, and a limitation of liability clause for consequential and other damages. Again, in *Mortenson Company, Inc. v. Timberline Software Corporation* (2000), Timberline's license agreement provided the usual warranty disclaimers, together with a disclaimer for damages or liability. When the plaintiff nonetheless brought suit for breach of express and implied warranties, alleging the software was defective, Timberline moved for summary judgment, arguing the limitation on consequential damages in the licensing agreement barred Mortenson's recovery. Moreover, Revised Article 2 tends to sanction this practice by purporting to exclude informational products from the scope of the UCC.

Warranties for Informational Products under UCITA

The Uniform Computer Information Transactions Act (UCITA, formerly UCC Draft Article 2B), is founded upon the conceptual framework for commercial transactions in Article 2 of the UCC, which regulates the sale of goods. UCITA creates a standard framework of rules applicable to software and other computer information licensing transactions. "Information" includes computer programs, "computer information" means information in electronic form, and "computer information transaction" includes license agreements (§ 102(35), (10), and (12)).

UCITA contains several innovative provisions drafted to accommodate issues unique to transactions in information. These provisions address such controversial questions as the validity of adhesion contracts, warranties for information products, problems associated with breach, and the remedies for breach. Other issues addressed by the provisions are express warranties (s. 402) and implied warranties of quiet enjoyment and noninfringement, merchantability and quality of the computer program's informational content, licensee's purpose, and system integration (ss. 403-5).

Although UCITA contains implied warranties that reflect those found in sales law, these warranties have been adjusted and expanded to meet the unique character of information products. For example, merchantability for mass-market licenses consists of five minimum performance standards, including the contract description, fitness for the ordinary purposes, and the functionality of a computer program (ss. 403-5). The warranty that the goods will be fit for purchaser's purpose is the same as in sales law if the transaction is to deliver a product; however, UCITA creates a standard to distinguish this warranty from a services contract. Although sales law has no implied warranty that services will give a result consistent with the transferee's purpose, UCITA warrants that the services will not fail of the purpose because of a lack of effort. Again, where necessary, UCITA extends the nature and scope of implied warranties, as in the case of the warranty that the system components will work in integration (s. 405).

In sum, warranties for informational products are still at a formative stage. Although two states have enacted UCITA (Maryland and Virginia), five states (Iowa, West

P1: pdb
JWBS001B-97.tex WL041/Bidgoli WL041-Bidgoli.cls November 10, 2005 10:51 Char Count= 0

Virginia, New York, Oregon, and Ohio) have enacted anti-UCITA "bomb shelter" legislation that would protect their residents from the application of UCITA in a transaction subject to the laws of states that have enacted it. Given the extent of the controversy, UCITA was significantly amended by NCCUSL in 2002 in response to substantive recommendations made by a Working Group on UCITA appointed by the American Bar Association. Absent statutory provisions, it is likely that courts will base their decision-making on the common law of contracts and the Restatement (Second) of Contracts as the case of *Specht* illustrates. Consequently, taking account of the problematic state of warranties for fitness, for purpose, and for merchantability of software and content, buyers would be well advised to seek warranties from the supplier wherever possible and to the extent feasible to ensure that the software will operate under certain conditions and that it will have the functionality the business needs.

CONSUMER PROTECTION ONLINE

Caveat Emptor

As consumer groups have argued, under the terms of UCITA it is relatively easy for the licensor to eliminate any warranty or representation in mass-market licenses. In fact, because of the strength and concentration of the software and content industries, there has been international interest in ensuring that consumers have adequate redress against defective products (Evans, 1999). The Organization for Economic Cooperation and Development (OECD) *Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999) are designed to help ensure that consumers are no less protected when shopping online than they are when they buy from local stores or order from catalogues. By setting out the core characteristics of effective consumer protection for online business-to-consumer transactions, the guidelines are intended to help eliminate some of the uncertainties that both consumers and businesses encounter when buying and selling online. The guidelines reflect existing legal protection available to consumers in more traditional forms of commerce; encourage private sector initiatives that include participation by consumer representatives; and emphasize the need for cooperation among governments, businesses, and consumers. Their aim is to encourage fair business, advertising, and marketing practices; clear information about an online business's identity, the goods or services it offers, and the terms and conditions of any transaction; a transparent process for the confirmation of transactions; secure payment mechanisms; fair, timely, and affordable dispute resolution and redress; privacy protection; and consumer and business education.

Choice of Law

Although the ability to market and sell products and services from a single site to an unlimited geographic market is one of the advantages of electronic commerce, it also poses a major challenge for consumer protection online (*American Libraries Ass'n. v. Pataki*, 1997). When transactions cross the jurisdictional boundaries defining legal communities, there must be a workable method of coordinating the rights and liabilities of the parties. Fair, timely, and affordable dispute resolution is not possible if consumers are unable to benefit from the protection they have come to expect. One of the key issues for policymakers is developing a practicable and reasonably predictable set of rules to determine which jurisdiction's laws will apply to consumer contracts and which courts will have the authority to adjudicate and enforce disputes. UETA and, to a lesser extent E-SIGN provide little guidance with respect to these issues. UETA provides, as a default rule, that an electronic record is deemed to be sent from the sender's place of business and to be received at the recipient's place of business (§15(d)) or residence (§15(d).) UCITA, which allows the choice of any U.S. forum (including a foreign one) for the convenience of the producer, is criticized for allowing a too flexible choice of law and forum in mass-market transactions to the detriment of consumer interests.

Insofar as the sale of goods (as distinct from information), is concerned, Revised Section 1-301 of the UCC represents a significant rethinking of the choice of law issues addressed in current UCC Section 1-105. Current law allows the parties to the transaction to designate a jurisdiction whose law is to govern, if the transaction bears a "reasonable relation" to that jurisdiction. Revised Article 1 deviates from this unified approach by providing different rules for consumer transactions than for "business to business" transactions. Revised Article 1 requires no such relationship between the transaction and the chosen jurisdiction, unless one of the parties to the agreement is a consumer. It proposes a choice of law rule that would afford greater autonomy to each party, but with certain safeguards to protect consumer interests. On the one hand, Revised Article 1-301 purports to allow vendors the ability to choose the law of any state to apply to their contracts. On the other hand, Revised Article 1-301(2) provides that a choice of law agreement cannot alter the applicability of a consumer protection law of the state in which the consumer habitually resides. Thus, if ComCo has its headquarters in New York, I am a resident of California, and I purchase a microwave oven from a ComCo store in Ohio, then a provision in the sales agreement subjecting all disputes to the law of Texas would not be binding because I am a consumer. However, if Comco purchased the microwave for resale from Panacook, located in North Carolina, and had it shipped directly to the California store, then a provision in the Comco-Panacook agreement subjecting all disputes to Texas law would be binding because neither party is a consumer.

Needless to say, the proposed choice of law rule has given rise to controversy concerning the scope of party autonomy on the part of both business and consumer interests (National Association of Manufacturers, 2004). Many businesses find the notion that they should be expected to comply with the various regulatory regimes in which consumers happen to be located expensive and unrealistic (Americans for Fair Electronic Commerce Transactions, 2004; National Conference of Commissioners on Uniform State Laws, 2001a). The revision is sufficiently problematic that none of the small number of states that have enacted Revised Article 1 to date has enacted Section

R1-301 as drafted. Virginia's version of Revised Article 1 (effective July 1, 2003) rejects the uniform version's choice of law provision, opting to retain the basis of former Section 1-105, which requires some reasonable relation between the state whose law the parties choose by agreement and the transaction the parties choose to subject to that law. In view of the novelty and potentially problematic nature of consumer contracts online, revised UCC Article 2 gives the courts the right to overrule the statute in contracts involving consumers. Hence, Revised §2-108(1)(b) is subordinate to any judicial decision "that establishes a different rule for consumers."

BEST PRACTICE FOR ONLINE CONTRACTS

The foregoing review of statute and case law has provided some pertinent indications as to how online vendors, in particular software vendors and content providers, might utilize clickwrap agreements to protect their rights and promote consumer confidence. In the absence of national standards and given the sometimes divergent decisions of the courts respecting these issues, online business should keep in mind three general criteria with regard to the enforceability of clickwrap and browsewrap agreements:

1. Agreements that are clear and conspicuous and require some proof of acceptance by the user are more likely to be enforced by the courts.
2. Browsewrap and clickwrap agreements potentially face challenges on two separate grounds: procedural challenges based on the manner in which the mutual assent is made and substantive challenges as to the terms of the agreement itself. Thus, even if the agreement is enforceable overall, particular terms might not be enforceable.
3. The enforcement of clickwrap and browsewrap agreements is likely to differ depending on the law in the jurisdiction where the contract is construed.

Consequently, when drafting an online agreement on behalf of the vendor, best practice involves two chief points:

1. To increase the site's chances of having any such agreement enforced against site visitors, the agreement should be set up so as to create a "contract." This means that, in addition to the issues about validity of consideration, there must be an offer that is set forth in the respective agreement, terms of service and, for the issues related to this chapter, a valid "acceptance" of the terms of that offer. Hence, there must be prominently displayed on the site, preferably on the home page, a link to the respective agreement in large, bold type. This link must take the visitor to the agreement, and there must be a mechanism whereby the visitor affirmatively clicks on an "I accept" button, having been given an opportunity to review the terms and conditions, before being able to proceed through the site. This latter procedure—blocking access to the site until there is an affirmative response from the visitor—is what the courts seem most likely to look for in determining whether there has been a valid acceptance. Equally, vendors should make sure that the buyer has the opportunity to reject the transaction upon review of the terms.
2. Vendors should make sure warranty disclaimers and limitations of damages are conspicuous by placing them in a large, bolded font and making sure that the purchaser does not have to scroll down to see them. Equally, it is not advisable to place additional terms where they can only be viewed through a "disclaimer" link or at another location on the Web site.

In summary, by ensuring that the terms and conditions are readily accessible, that the purchaser has certain clear rights upon receipt and review of these provisions, and not least by keeping records to prove assent, vendors can minimize the possibility that a court may conclude that they are unenforceable.

Even if best practice is followed, it is still possible that a purchaser may dispute his or her consent to terms and conditions that appear in a shrinkwrap or clickwrap agreement. In such an event, in an attempt to bring the dispute settlement into familiar home territory, consider adding an arbitration clause. Alternatively, an agreement might attempt to invoke laws more favorable to software and content providers, such as those of California, or to have recourse in a choice of law clause to the law of those states where UCITA applies such as Virginia.

Given the unsettled state of the law, whether you are an individual user or in a business, software licenses may need more careful attention than simply clicking "I accept." Falling into the clickwrap trap can leave buyers vulnerable to costly upfront fees and products that are not fit for the intended purpose. Those in business would be well advised to protect their company's intellectual property by taking the time to negotiate all software licenses, even those involving off-the-shelf software. Readers now cognizant of the uncertain state of the law, who take the time to read the entire clickwrap agreement, may well decide they want to buy on very different terms!

CONCLUSION

The law relating to the enforceability of contracts online is still in its formative stages. Early legislative intervention in the form of electronic signature legislation has largely accomplished two goals: first, it has removed the initial barriers to e-commerce, and second, it has promoted the uptake of electronic commerce by helping establish the "trust" and the "predictability" needed by the parties if they are to enter into contracts online. Likewise, the courts have followed suit in seeking to validate the clickwrap and browsewrap agreements used by vendors to distribute their goods online. Yet, now that in the United States alone there are 46 enactments of electronic signature legislation, not to mention the national variations that exist worldwide, the very predictability that governments are seeking to establish is at risk. Consequently, with the aim of continued harmonization, the United Nations Commission on International Trade Law (UNCITRAL) is constructing a *Draft Convention On [International] Contracts Concluded Or Evidenced By Data Messages* (2002). It

includes provisions dealing with the substantive rights and obligations of the parties in the context of contract formation by electronic means.

In sum, the continued development of electronic commerce depends on how problems are resolved relating to the formation and enforceability of contracts online. Rules regarding offer and acceptance, place of formation, and certainty of terms are still not perfectly transferable to the online environment. As far as the individual parties are concerned, those who contract autonomously and in the course of an ongoing business relationship can simply agree to the particular rules that are to govern their transactions. However, where standard form, mass market contracts are concerned, given the failure of UCITA to gain widespread acceptance, it remains largely up to the courts to adapt the law of contract to the online environment.

GLOSSARY

Assent/Consent In law, the active acquiescence or silent compliance by a person legally capable of consenting (see age of consent). It may be evidenced by words or acts or by silence when silence implies concurrence. Actual or implied consent is necessarily an element of every contract and every agreement. In criminal charges, the consent of the party injured (if not obtained by fraud or duress) is a defense for the accused, unless a third party or the state is injured.

Browsewrap license A "browsewrap agreement" appears on a web site, but does not require the user to take any action to express consent. The terms of the agreement are displayed to users only if they click on the hyperlink that brings up the "terms and conditions" page.

Clickwrap License A window containing the terms of a clickwrap agreement commonly appears on the downloading, installation, or first use of a software application. The user is asked to click either "I agree" or "I do not agree." If the user does not agree, the process is terminated.

Contract For a contract to be valid, both parties must indicate that they agree to its terms. This is accomplished when one party submits an offer that the other accepts within a reasonable time or a stipulated period. If the terms of the acceptance vary from those of the offer, that "acceptance" legally constitutes a counteroffer; the original offering party may then accept it or reject it. At any time before acceptance, the offer may be rescinded on notice unless the offering party is bound by a separate option contract not to withdraw.

Copyright A property right by an author in an original work that has been fixed in a tangible medium, including literary, musical, artistic, photographic, or film works. The holder of a copyright has the exclusive right to reproduce, distribute, perform, and display the work.

Electronic Contract An electronic contract is an agreement created and "signed" in electronic form—in other words, no paper or other hard copies are used.

Electronic Signature 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.

Fair Use An exception under the U.S. Copyright Act that allows one who does not own a copyright to make "fair use" of the copyrighted work for such purposes as criticism, comment, news reporting, teaching, scholarship, or research without being liable for copyright infringement.

Internet The international computer network linking together thousands of individual networks at military and government agencies, educational institutions, nonprofit organizations, industrial and financial corporations of all sizes, and commercial enterprises (called gateways or service providers) that enable individuals to access the network.

Law Merchant (or *Lex Mercatoria*). Originally a body of rules and principles relating to merchants and mercantile transactions, developed by merchants themselves for the purpose of regulating their dealings. The law merchant owed its origin to the fact that the civil law was not sufficiently responsive to the growing demands of commerce, as well as to the fact that trade in medieval times was in the hands of those who might be termed cosmopolitan merchants, who wanted a prompt and effective jurisdiction.

License Licensing is a branch of the law of contracts. The contract is a specific form of agreement and strictly speaking embodies a license; that is, a permission from an owner of a right given to another to use part of that right. The other side of the contract is the obligation assumed by the receiver of the permission (i.e., the licensee) in return for the permission.

Online The state in which a computer is connected to another computer or server via a network; in other words, a computer communicating with another computer.

CROSS REFERENCES

See *Copyright Law; Digital Signatures and Electronic Signatures; Internet Basics; Legal, Social and Ethical Issues of the Internet; The Legal Implications of Information Security: Regulatory Compliance and Liability.*

REFERENCES

Afuah, A., & Tucci, C. (2000). *Internet business models and strategies*. Boston: McGraw-Hill.

Americans for Fair Electronic Commerce Transactions. (2004). *Proposed UCITA-related legislation*. Retrieved September 15, 2004, from http://www.affect.ucita.com/Legislation.htm

American Libraries Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y., 1997).

Applied Info. Mgmt. Co. v. Icart, 976 F. Supp. 149, 155 (E.D.N.Y. 1997).

Bonito Boats, Inc. v. Thunder Craft Boats, Inc. 489 U.S. 141, 109 S.Ct. 971 (U.S.Fla., 1989).

Bowers v. Baystate Technologies Inc., 320 F.3d 1317 (C.A.Fed. (Mass.), 2003).

Caspi v. Microsoft Network, L.L.C., 732 A.2d 528 (N.J.Super.A.D., 1999).

Comb v. PayPal Inc., 218 F.Supp.2d 1165 (N.D.Cal., 2002).

Commission of the European Communities (1999). *Proposal for a Directive of the European Parliament and of the Council on the Community Framework for Electronic Signatures*.

CompuServe, Inc. v. Patterson, 89 F.3d 1257 (C.A.6 (Ohio), 1996).

Corinthian Pharmaceutical Systems v. Lederle Labs, 724 F. Supp. 605 (S.D. Ind. 1989).

Digital Millennium Copyright Act framework Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

Evans, G. E., (1999). Opportunity costs of globalizing information licenses. *Fordham University Journal of Intellectual Property, Arts and Entertainment Law, 10*(1), 267.

Federal Trade Commission. (2001, June). *Report to Congress on The Electronic Signatures In Global And National Commerce Act: The consumer consent provision in Section 101(c)(1)(C)(ii)*. Retrieved September 15, 2004, from http://www.ftc.gov/reports/#2001

Feist Publications v. Rural Telephone Service Co, 111 S.Ct. 1282 (U.S.Kan., 1991).

Forest v. Verizon Communications Inc. 2002 D.C. App. LEXIS 509.

Hill v. Gateway, Inc., 105 F.3d 1147 (C.A.7 (Ill.), 1997).

I Lan Systems v. Netscout Service Level Corp., 183 F.Supp.2d 328 (D.Mass., 2002).

I-Sys Inc. v. Softwares Inc., Civil No. 02-1951, 2004 WL 742082 (D. Minn. 2004).

Kewanee Oil Co. v. Bicron Corp. U. S. Supreme Court 416 U.S. 470, 94 S.Ct. 1879 (U.S. Ohio 1974).

M.A. Mortenson Co., Inc. v. Timberline Software Corp., 998 P.2d 305 (Wash., 2000).

Market Development Corp. v. Flame-Glo Ltd., 1990 WL 116319 (E.D. Pa. August 8, 1990).

National Association of Manufacturers. (n.d.). *Industry concerns about Final Article 2 Revisions*. Retrieved September 15, 2004, retrieved June 5, 2005 from http://www.nam.org/s_nam/doc1.asp?CID=200173&DID=223242

National Conference of Commissioners on Uniform State Laws. (2001a). *Drafts of Uniform and Model Acts: Uniform Commercial Code, Revision, Article 1*. Retrieved September 15, 2004, from http://www.law.upenn.edu/bll/ulc/ulc.htm

National Conference of Commissioners on Uniform State Laws. (2001b). *Uniform Computer Information Transactions Act (formerly Uniform Commercial Code Draft Article 2B)*. Retrieved September 15, 2004, from http://www.law.upenn.edu/bll/ulc/ucita/ucita01.htm

National Conference of Commissioners on Uniform State Laws. (2002). *Drafts of Uniform and Model Acts: Uniform Commercial Code, Revision, Article 2*. Retrieved September 15, 2004, from http://www.law.upenn.edu/bll/ulc/ulc.htm

Nimmer, R. (1998). Breaking barriers: The relationship between contract and intellectual property law. *Berkeley Tech LJ, 13*, 827.

Organization for Economic Cooperation and Development (OECD). (1999). *Guidelines for consumer protection in the context of electronic commerce*. Retrieved September 15, 2004, from http://www1.oecd.org/publications/e-book/9300023E.PDF

Pollstar v. Gigmania Ltd., 170 F.Supp.2d. 974 (E.D. Cal. 2000)

ProCD v. Zeidenberg, 86 F.3d 1447 (C.A.7 (Wis.), 1996)

Register.com Inc. v. Verio Inc., 356 F.3d 393 (C.A.2 (N.Y.), 2004)

Reichman, J. R. (1999). Privately legislated intellectual property rights: Reconciling freedom of contract with public good uses of information. 147 U. Pa. L. Rev. 875.

Rosenfeld v. Zerneck, 776 N.Y.S.2d 458 (N.Y.Sup., 2004).

Shattuck v. Klotzbach, 2001 Mass. Super. LEXIS 642 (December 11, 2001).

Smedinghoff, T. J. (2002). *The legal requirements for creating secure and enforceable electronic transactions*. Retrieved September 15, 2004, from http://www.bakernet.com/ecommerce/etransactionsarticle.pdf

Specht v. Netscape Communications Corp., 150 F.Supp.2d 585 (S.D.N.Y., 2001), aff'd.–306 F.3d 17 (C.A. 2 (N.Y.) 2002).

State Farm Mutual Auto. Ins. Co v. Bockhorst, 453 F.2d 533 (C.A.10, 1972).

Ticketmaster Corp. v. Tickets.com, Inc., 2Fed.Appx. 741 (C.A.9 (Cal.) 2001).

U.S. v. Eisenberg, 807 F.2d 1446 (8th Cir. 1986)

U.S. v. Grande, 620 F.2d 1026 (4th Cir. 1980), cert. denied, 449 U.S. 830, 919 (1980).

United Nations Commission on International Trade Law (UNCITRAL). (1996). *Model law on electronic commerce*. Retrieved September 15, 2004, from http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm

United Nations Commission on International Trade Law (UNCITRAL). (2002). *Preliminary draft convention on [international] contracts concluded or evidenced by data messages*. Retrieved September 15, 2004, from http://www.law.gov.au/agd/seclaw/electronicpaper.html

U.S. Department of Commerce. (2003). Information technology producing industries—Hopeful signs in 2003. *Digital Economy, 2003*. Retrieved September 15, 2004, from https://www.esa.doc.gov/reports/DE-Chap1.pdf

Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 261 (C.A. 5 (La.), 1988).

White House. (1997, July 1). *A framework for global electronic commerce*. Retrieved September 15, 2004, from http://www.technology.gov/digeconomy/framewrk.htm