# "ONLINE CONTRACTING IN CYBERSPACE"

BY

Stephen H. LaCount

## 1. MILLENNIUM DIGITAL COMMERCE ACT: OVERVIEW

A. On June 30, 2000, the United States enacted the Millennium Digital Commerce Act, also known as the Digital Signatures or E-SIGN legislation ("E-SIGN'). E-SIGN is the most significant e-commerce online contracting legislation adopted at the federal level to date. By granting nationwide legal recognition to electronic signatures and records in the United States, E-SIGN gives the same legal effect to electronic signatures, contracts, and records that is accorded to paper and ink signatures, contracts and records and contains consumer protection measures requiring consumer notice and consent before electronic records can be binding. With some exceptions, E-SIGN took effect on October 1, 2000. For record retention requirements imposed by federal or state statutes or agency rules, E-SIGN will take effect on March 1, 2001.

B. Prior to E-SIGN, there had been little uniformity at the state level. Some states authorized electronic signatures only in limited circumstances; others authorized electronic signatures in broader circumstances (California has had an electronic signatures law since 1995). In 1999, the National Conference of Commissioners on Uniform State Laws in the United States developed and approved the Uniform Electronic Transactions Act ("UETA"), a model law which had been adopted in 22 states by August, 2000. However, state adoption of UETA was not accomplished in a uniform manner. E-SIGN was specifically designed and implemented to promote uniform nationwide legal standards.

C. E-SIGN establishes a general rule that a signature, contract, or other record in electronic form will not be denied legal effect solely because it is in electronic form or an electronic signature was used in forming the agreement. "Electronic record" is defined very broadly to cover any record created, generated, sent, communicated, received or stored by electronic means and applies to any transaction in or affecting interstate or foreign commerce. "Transaction" is also defined broadly to include any action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons.

D. E-SIGN provides that an electronic record or contract will be legally binding provided that the electronic record or contract (i) accurately reflects the information contained in the contract or record, and (ii) remains accessible to all persons entitled by law to have access to it and capable of being reproduced. Even if an existing law specifically requires that a record or contract be retained in its original form, an electronic record will suffice as long as it meets the requirements of accuracy and accessibility. Similarly, if the law requires a check to be retained, that requirement will be satisfied by retaining an electronic record of information on the front and back of the check that is accurate and accessible. If an existing law requires a signature to be notarized, an electronic signature will satisfy that requirement as long as all the legally required information is attached to or associated with the electronic record.

E. E-SIGN sets forth a series of notice and consent requirements designed to protect consumers in business-to-consumer transactions. *(These requirements do not apply to business-to-business transactions).* For the consumer's consent to be valid, the consumer must receive a "clear and conspicuous statement" informing the consumer of (i) any right or option to have the record provided in non-electronic form, of the consumer's right to withdraw consent to maintain the record in electronic form; (ii) the consequences of such withdrawal (such as penalties or termination of the business relationship); (iii) whether the consent applies only to a particular transaction or to identified types of records that may be provided during the parties' relationship; (iv) the procedures the consumer must use to withdraw consent and to update information needed to contact the consumer electronically; (v) how the consumer may obtain a paper copy of an electronic record and whether any fee will be charged for such copy; and (vi) the software and hardware required to access and retain the electronic records. E-SIGN further requires that the consumer either consent or confirm consent electronically in a way that "reasonably demonstrates" that the consumer can access the information electronically. If a consumer withdraws consent, the withdrawal operates prospectively only, and will not alter the legal effect of any electronic records made or provided before the consent is withdrawn.

F. E-SIGN's provisions <u>do not</u> apply to requirements for use of written records or signatures for certain types of documents such as wills, codicils, testamentary trusts, matters relating to adoption, divorce, or other matters of family law, court orders or notices of other official court documents, notices of cancellation or termination of utility services, notices of cancellation or termination of health insurance or life insurance benefits (excluding annuities), and notices of product recalls or material product failures that pose a risk of danger to health or safety.

G. E-SIGN generally preempts inconsistent state laws requiring written signatures and records (i.e., E-SIGN establishes a national "floor of recognition"). To the extent that a state adopts the UETA, or other legislation consistent with E-SIGN, state law will apply. While the federal government and states are free to adopt state laws that go further than E-SIGN and permit greater use of electronic signatures and records, state laws can not restrict the use of electronics signatures and records where E-SIGN permits their use.

H. To encourage international adoption of the standards in E-SIGN, the Act directs the U.S. Commerce Department to promote the acceptance and use of electronic signatures on an international basis consistent with E-SIGN and to eliminate or reduce impediments to digital signatures to facilitate the growth of e-commerce.

## 2. UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT: OVERVIEW

A. In late 1999, the National Council of Commissioners on Uniform Laws sponsored the Uniform Computer Information Transactions Act ("UCITA") as a model law to be adopted by the States (as of April 2000, UCITA has been enacted by Virginia and Maryland and is currently being considered by a number of other states). UCITA is a contract law "cyberspace commercial statute" which is designed to clarify the law governing "computer information transactions". UCITA draws on common law, Article 2 of the UCC, and commercial practice to provide guidance with regard to drafting and presenting computer information transaction agreements, including "mass market license" agreements, so as to make them enforceable. But UCITA is not a "general purpose" statute for licensing transactions, and its scope extends only to "computer information transactions".

B. UCITA will apply to many types of transactions in the software and online industries where standardized agreements are used. Section 103 of UCITA defines "computer information transactions" as agreements (or the performance of agreements) to create, modify, transfer or license "computer information" or "informational rights" in computer information, including (i) contracts to develop or create: (i) software, digital multimedia works and other computer information, (ii) transactions involving the distribution or use of computer programs, access to or information from a computer system (including the Internet), and (iii) contracts for data processing or data analysis of computer information. UCITA excludes print and other forms of informational distribution, and transactions in the "traditional core businesses of non-digital information industries (e.g., print, motion picture, broadcast, sound recordings). Other specifically enumerated limitations on the scope of UCITA include financial services transactions, contracts to create, perform or perform in motion pictures, sound recordings, musical works, or phonorecords, or programming provided by broadcast, satellite, or cable or similar systems, compulsory licenses, employment contracts, contracts where the computer information component is insignificant, and contracts where the subject matter is within the scope of Articles 3 through 8 of the Uniform Commercial Code.

C. For mixed transactions (*i.e.,* those including computer information and other subject matter), the extent to which UCITA applies will depend on whether the other subject matter of the transaction fall within the scope of the Uniform Commercial Code (in which case the UCC will apply to such subject matter). If the other subject matter is not within the scope of the UCC, UCITA will apply only to the computer information or informational rights in the transaction. In addition to such default rules, UCITA also provides a means for parties to contractually agree to "opt-in" or "opt-out" of the act with respect to certain types of transactions.

D. UCITA will not apply if preempted by federal law and does not alter intellectual property or other information rights laws. UCITA also will not apply to the extent is violates fundamental public policy and may in many cases be "trumped" by state consumer protection statutes.

E. The most noteworthy thrust and future significance of UCITA is probably the framework established by the Act to enable use and enforceability of shrinkwrap and clickwrap agreements. UCITA builds upon principles enunciated by the Seventh Circuit in *ProCD,* and other similar case precedents, by favoring contact formation based on a licensee's affirmatively assenting to the terms of a standardized agreement after having an opportunity to review -and reject-its terms, and providing for an opportunity to return and receive a refund if the terms are rejected. It also recognizes the advent of the Internet and electronic-commerce transactions where contracting parties may conduct transactions via Web sites and other remote or automatic means. Enforceability of standardized shrinkwrap and clickwrap agreements in consumer transactions are addressed via the "mass-market license" defined in the Act as a standard form used in a "mass-market transaction."

F. Under the provisions of UCITA, a party adopts the terms of a mass-market license only if the party agrees to the license, including by "manifesting assent", before or during the party's initial performance or use of or access to the information. A party manifests assent if, acting with knowledge of, or after having an opportunity to review the record or term or a copy of it, the party "authenticates the record or term with intent to adopt or accept it"; or "intentionally engages in conduct or makes statements with reason to know that the other party or its electronic agent may infer from the conduct or statement that the person assents to the record or term".

G. A party must have an opportunity to review the mass-market license as a condition precedent to a party's manifesting assent under UCITA. In the context of Internet-based transactions where a licensor makes computer information available via an Internet site or by similar means, the requirement that there be an opportunity to review is satisfied if the licensor (i) makes the standard terms of the license readily available for review by the licensee; before the information is delivered or the licensee becomes obligated to pay, whichever occurs first," and (ii) does not take affirmative acts to prevent printing or storage of the standard terms for archival or review purposes by the licensee.

H. The enactment of UCITA has proven to be controversial and was opposed by over 20 state attorneys general ( including some of the attorneys general involved in the Microsoft ligitation), the Federal Trade Commission and a number of library organizations. The concerns voiced by these organizations focused on whether the provisions of UCITA will enable software vendors (e.g., Microsoft) to impose "unfair" mass-market or shrinkwrap/click-on licenses on consumers, undercut fair use, preservation, and the unhindered use of works in the public domain, and prevent reverse engineering even in cases of interoperability.

## 3. ENFORCEABILITY OF ONLINE CONTRACTS: A PRACTICAL OVERVIEW

A. With the rapid growth of e-commerce and web-based delivery models, enforceable online agreements have become a key component to building a strong e-commerce legal infrastructure. While the practice of using of shrinkwrap and clickwrap agreements to bind consumers to contractual terms determined by sellers and licensors is now common or "ubiquitous" in the software and online industries, the number of cases addressing the enforceability of such agreements is still relatively small.

B. The principal court rulings are the Seventh Circuit's 1996 *ProCD, Inc. v. Zeidenberg* decision (holding that shrinkwrap licenses are enforceable unless their terms are "objectionable on grounds applicable to contracts in general") and its 1997 *Hill v. Gateway* decision (holding that a contract included in a Gateway computer box would be enforceable where the contract stated that its terms would govern the relationship between Gateway and the purchaser unless the purchaser returned the computer system within thirty days – and the purchaser failed to do so). A copy of these leading cases is attached to this outline. The trend among courts considering the issue of validity has generally been to uphold the enforceability shrinkwrap and on-line clickwrap agreements.

C. Recent cases have enforced various forms of online agreements. Most courts have found click-wrap agreements to be valid and enforceable. Click-wrap agreements are widely considered to be more enforceable than "shrink-wrap" which are entered into based on the licensee opening the software products' packaging or failing to return the product within a specified period, typically 7 to 30 days. Contract formation is the click-wrap agreement context has the added positive element of an affirmative assent as opposed to the failure to act. However, it should be kept in mind that if such agreements are too one-sided or overbearing (or contain unusually harsh terms), there is always the possibility that a court could rule that a click-wrap agreement, even if assented to, is unconscionable and unenforceable. Accordingly, click-wrap agreements should provide a clear and simple mechanism allowing the consumer to return the products for a refund within a reasonable period of time. It is also recommended that the terms and conditions of the agreement be available for inspection in "hard copy" at specified locations.

D. Click-wrap agreement users should establish a policy of maintaining records of the disclaimers and contract terms contained on their websites, including any changes made to such terms over time. A prominent notice should be displayed on the opening page of the website instructing users to review the terms and conditions of usage and alerting users to changes in the terms as they occur.

E. Well-drafted online service or use agreements should be designed and implemented as an important strategy for managing the risks of operating an e-commerce website. These agreements are generally enforceable and critical to limiting the jurisdictional exposure of e-commerce merchants who would otherwise be subject to being hauled into court wherever a customer may be located (i.e., include venue-selection and governing law provisions, limitation of liability, and other provisions to limit legal exposure and minimize legal risks).

F. Post privacy policies, spam policies and other use policies at the website (see sample attached).

## Prohibited Uses Policy

The following actions are defined by EROGO as “system abuses” and are strictly prohibited under the Agreement. The examples named in this list are not exhaustive and are provided solely for guidance to Customers using the Services. EROGO reserves the right to suspend, revoke or otherwise terminate provision of service to any Customer willfully disregarding this policy.

A user will not, nor will a user permit any other persons using EROGO's Service or online facilities to do any of the following:

- Engage in “Spamming” (the sending of unsolicited commercial e-mail messages).

- Use EROGO's services or facilities for any illegal purposes.

- Misappropriate or infringe the intellectual property rights of others, including without limitation the unauthorized posting of copyrighted material, using trademarks of others without appropriate permission or attribution, or disclosing trade secret information of others in violation of confidentiality obligations.

- Invade or otherwise violate the privacy rights of others, including without limitation collecting and distributing information about Internet users without their consent, except as permitted by law.

- Transmit, post or host defamatory, harassing, abusive, or libelous materials or take any similar actions.

- Omit, delete, forge or misrepresent transmission information, including headers, return addressing information and IP addresses or take any other actions intended to cloak such user's or any other users' identity or contact information.

- Assist or permit any persons in engaging in any of the activities described above.