2000

UCITA: THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT

Michael J. Lockerby

Follow this and additional works at: http://scholarship.richmond.edu/jolt

Part of the Computer Law Commons, Intellectual Property Law Commons, and the Privacy Law Commons

Recommended Citation


Available at: http://scholarship.richmond.edu/jolt/vol7/iss2/7

This Symposium Information is brought to you for free and open access by UR Scholarship Repository. It has been accepted for inclusion in Richmond Journal of Law and Technology by an authorized administrator of UR Scholarship Repository. For more information, please contact scholarshiprepository@richmond.edu.
Volume VII, Issue 2,
Fall 2000

UCITA:
THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT
by Michael J. Lockerby[*]


TABLE OF CONTENTS

I. INTRODUCTION

II. MAKING PAPERLESS CONTRACTS ENFORCEABLE
   A. Admissibility = Enforceability
   B. The Statute of Frauds in Cyberspace
   C. Changes Resulting from UCITA

III. ENFORCING CONTRACTS
   A. Traditional Principles of Jurisdiction In American Courts
B. Mere Advertisement or Solicitation for Sale of Goods and Services on the Internet Probably Insufficient to Establish Jurisdiction

C. What Satisfies the "Something More" Necessary to Show "Purposeful Availment" and Therefore Jurisdiction?

D. Comparative Law

E. Choice of Law and Forum Clauses

F. Effect of UCITA

IV. THE USE OF COMPUTER CRIMES LAWS TO OBTAIN JURISDICTION

A. Advantages of Invoking Protections of Computer Crimes Laws

B. Federal Computer Crimes Legislation

C. U.S. Federal Electronic Communications Privacy Act

D. State Computer Crimes Laws

E. E-Mail As Computer Crimes

F. Comparative Law

G. Is Self-Help a "Computer Crime"?

V. REMEDIES UNDER UCITA

A. Available Remedies

B. Special Rules for Licenses/Self-Help

I. INTRODUCTION

From the heated rhetoric of both proponents and opponents of UCITA, one would think that UCITA represented a radical change from current law. From the standpoint of this practitioner, however, UCITA represents more of an evolutionary than a revolutionary change in the law. In at least three critical areas, the enforceability of "paperless contracts," dispute resolution, and "self-help" remedies, UCITA is arguably consistent with current law or at least the trend of current law. Indeed, the main inconsistency between UCITA and current law is that current law is at times inconsistent. From the standpoint of most businesses, certainty is preferable to uncertainty. Therefore, a rule of law that is consistently bad may well be preferable to a rule that -- while theoretically good -- is applied so inconsistently that the rights and obligations of the parties are in doubt. In any event, this paper compares current law with the changes resulting from UCITA for
the purpose of assessing just how significant a change UCITA really represents.

II. MAKING PAPERLESS CONTRACTS ENFORCEABLE

A. Admissibility = Enforceability

1. Obviously, whether a contract is enforceable becomes an issue only when there is a contractual dispute that may be headed to litigation. At that point, the contract will be enforceable only if it is admissible. Long before the adoption of UCITA, the federal courts have allowed, and in some cases required, the use of electronic records in litigation.

2. It is well-settled that something does not have to be in tangible, written form to constitute a "document." For example, in Williams v. Dep't of Veterans Affairs [1] the U.S. Court of Appeals for the Fourth Circuit [2] held that draft letters and reports stored in electronic form are "records" within the meaning of the Privacy Act of 1974. [3]

3. The Federal Rules of Civil Procedure define "documents" to include "writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form . . . ." [4]

4. The Federal Rules of Civil Procedure not only permit litigants to produce records in electronic form, they sometimes require litigants to do so.

   a. In National Union Elec. Corp. v. Matsushita Elec. Indus. Co. [5] the court ordered the plaintiff to create a digital version of database reports that it had produced in hard copy form so they could be analyzed via computer.

   b. In Crown Life Ins. Co. v. Craig [6] the U.S. Court of Appeals for the Seventh Circuit [7] held that "Rule 34 contemplates that when data is in an inaccessible form, the party responding to the request for documents must make the data available."

5. Litigants who fail to preserve data in electronic form once they are notified to do so for purposes of litigation face severe sanctions.

   a. In William T. Thompson Co. v. Gen. Nutrition Corp. [8] the court-ordered sanctions for GNC's deletion of electronic records after it had been ordered to preserve its business records included striking its answer to the complaint, entering a default judgment against it, and dismissing its complaint in related litigation. [9]

B. The Statute of Frauds in Cyberspace

1. Traditionally, a writing is required to evidence an enforceable contract. The Uniform Commercial Code requires a "writing" that has been "signed" by the person against whom enforcement is sought for a contract for the sale of goods at a price of
a. "'Writing' includes printing, typewriting or any other intentional reduction to tangible form." [11]

b. "'Signed' includes any symbol executed or adopted by a party with present intention to authenticate a writing." [12]

2. In electronic commerce transactions, there may not be a hard copy of a written contract, and it may not have been signed by anyone. This commercial reality raises the issue of when there has been a "written" offer and acceptance sufficient to establish a binding contract.

3. In the United States, the federal courts have recently begun to recognize the enforceability of "clickwrap" agreements whereby acceptance of an offer is indicated by typing or clicking. For example, in *CompuServe v. Patterson* [13] the U.S. Court of Appeals for the Sixth Circuit [14] held that the defendant had entered into a written agreement with CompuServe (and was therefore subject to jurisdiction in Ohio, whose law governed the contract) by typing "Agree" at various points throughout the online agreement with which CompuServe had presented it. [15]

4. Decisions such as *CompuServe* are consistent with both current law and pending proposals that would clarify that a handwritten signature is just one of many ways of indicating acceptance of an offer.

   a. Under the *current* Uniform Commercial Code (the "UCC"), "(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 a contract." [16] This is consistent with the Restatement of Contracts, Section 19 of which states "the manifestation of assent may be made wholly or partly by written or spoken words or by other acts or by a failure to act." [17]

   b. A new U.C.C. Article 2B, proposed by the National Conference of Commissioners on Uniform State Laws and the American Law Institute, would clarify, in the context of electronic commerce transactions, the traditional requirement of a writing is not necessary to manifest assent:

   "Manifesting assent does not require a signature, any specific type of language or conduct, or any formalities. It can be shown by an authentication, by any conduct including use or other performance with respect to the subject matter, or by words." [18]

5. In both the United States and internationally, "digital signature" statutes provide that, if authenticated in accordance with statutory provisions, an electronic signature is entitled to as much binding effect as a written one.

   a. Revised Articles 2 and 2A and proposed Article 2B of the Uniform Commercial Code substitute the term "authenticate" for the requirement of a signature.
i. The term "authenticate" is defined as:

"to sign, execute or adopt a symbol or sound, or encrypt or process a record in whole or part, with intent by the authenticating person to: (A) identify that person; (B) adopt or accept a record or term that contains the authentication or to which a record containing the authentication refers; or (C) attest to the integrity of a record or term that contains the authentication or to which a record containing the authentication refers." [19]

ii. Proposed Article 2B specifically provides that "a record or authentication may not be denied legal effect, validity, or enforceability solely on the ground that it is in electronic form." [20] The purpose of this section is "to avoid any uncertainty about the efficacy of electronic records and signatures under state law as they apply to transactions covered by Article 2B." [21]

b. The Uniform Electronic Transactions Act ("UETA"), proposed by the National Conference of Commissioners on Uniform State Laws, would similarly ensure the enforceability of electronic contracts.

i. UETA equates an "electronic record" [22] with a "writing":

"(a) A record may not be denied legal effect, validity or enforceability solely because it is an electronic record. (b) If a rule of law requires a record to be in writing, or provides consequences if it is not, an electronic record satisfies that rule." [23]

ii. UETA also validates "electronic signatures" [24] for purposes of the Statute of Frauds:

"(a) A signature may not be denied legal effect, validity, or enforceability solely because it is in the form of an electronic signature.

(b) If a rule of law requires a signature, or provides consequences in the absence of a signature, the rule of law is satisfied with respect to an electronic record if the electronic record includes an electronic signature." [25]

c. The first digital signature statute in the United States, which was adopted in Utah in 1995, provided a model for subsequent enactments
i. The "digital signature" is actually encryption of an electronic message which allows the recipient to verify its sender.

ii. The verification is accomplished by a third party known as a "certification authority."

iii. Under the Utah statute, a digitally signed message satisfies the requirement of a "writing" and a "signature" if it has been verified by a licensed certification authority. [26]

iv. In November 1997, Utah licensed Digital Signature Trust Company to provide digital signature authentication and certification services to business and government. This was the first time in the world a government had licensed a "certification authority." [27]

d. Germany is among the countries with a similar Digital Signature Act.

i. Under the German Civil Code, a writing is not required for there to be an enforceable contract.

ii. The Digital Signature Act provides for a "digital signature" whereby digitized data intended for electronic transmission is sealed and labeled so that the recipient can verify the sender's authenticity and determine whether the data has remained unchanged after application of the digital signature. [28]

iii. This obstacle can be overcome by procedural provisions allowing for production of evidence by judicial inspection.

C. Changes Resulting from UCITA

1. Key Concepts

   a. Record = Document

   
   "(54) 'Record' means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." [29]

   b. Authenticate = Signature

   "(6) 'Authenticate' means (i) to sign or (ii) with the intent to sign a record, to execute or adopt an electronic symbol, sound, message, or process referring to, attached to, included in, or logically associated or linked with, that record." [30]
2. Manifesting Assent

"(a) A person manifests assent to a record or term if the person, acting with knowledge of, or after having an opportunity to review the record or term or a copy of it:

(1) authenticates the record or term with intent to adopt or accept it; or

(2) 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.

(b) An electronic agent manifests assent to a record or term if, after having an opportunity to review it, the electronic agent:

(1) authenticates the record or term; or

(2) engages in operations that in the circumstances indicate acceptance of the record or term.

(c) If this chapter or other law requires assent to a specific term, a manifestation of assent must relate specifically to the term.

(d) Conduct or operations manifesting assent may be proved in any manner, including showing that a person or an electronic agent obtained or used the information or informational rights and that a procedure existed by which a person or an electronic agent must have engaged in the conduct or operations in order to do so. Proof of compliance with subsection (a) (2) is sufficient if there is conduct that assents and subsequent conduct that reaffirms assent by electronic means." [31]

3. Relationship With Other Laws

"(d) If a law of this Commonwealth in effect on the effective date of this chapter applies to a transaction governed by this chapter, the following rules apply:

(1) A requirement that a term, waiver, notice, or disclaimer be in a writing is satisfied by a record.

(2) A requirement that a record, writing, or term be signed is satisfied by an authentication.

(3) A requirement that a term be conspicuous, or the like, is satisfied by a term that is conspicuous under this chapter.

(4) A requirement of consent or agreement to a term is satisfied by a manifestation of assent to the term in accordance with this chapter." [32]
4. Enforceability of Electronic Records

"(a) A record or authentication may not be denied legal effect or enforceability solely because it is in electronic form.

(b) This chapter does not require that a record or authentication be generated, stored, sent, received, or otherwise processed by electronic means or in electronic form.

(c) In any transaction, a person may establish requirements regarding the type of authentication or record acceptable to it.

(d) A person that uses an electronic agent that it has selected for making an authentication, performance, or agreement, including manifestation of assent, is bound by the operations of the electronic agent, even if no individual was aware of or reviewed the agent's operations or the results of the operations." [33]

5. Proof and Effect of Authentication

"(a) Authentication may be proven in any manner, including a showing that a party made use of information or access that could have been available only if it engaged in conduct or operations that authenticated the record or term.

(b) Compliance with a commercially reasonable attribution procedure agreed to or adopted by the parties or established by law for authenticating a record authenticates the record as a matter of law." [34]

6. Contract Formation

"(a) A contract may be formed in any manner sufficient to show agreement, including offer and acceptance or conduct of both parties or operations of electronic agents which recognize the existence of a contract.

(b) If the parties so intend, an agreement sufficient to constitute a contract may be found even if the time of its making is undetermined, one or more terms are left open or to be agreed on, the records of the parties do not otherwise establish a contract, or one party reserves the right to modify terms.

(c) Even if one or more terms are left open or to be agreed upon, a contract does not fail for indefiniteness if the parties intended to make a contract and there is a reasonably certain basis for giving an appropriate remedy.

(d) In the absence of conduct or performance by both parties to the contrary, a contract is not formed if there is a material disagreement about a material term, including a term concerning scope.

(e) If a term is to be adopted by later agreement and the parties intend
not to be bound unless the term is so adopted, a contract is not formed if the parties do not agree to the term. In that case, each party shall deliver to the other party, or with the consent of the other party destroy, all copies of information, access materials, and other materials received or made, and each party is entitled to a return with respect to any contract fee paid for which performance has not been received, has not been accepted, or has been redelivered without any benefit being retained. The parties remain bound by any contractual use term only with respect to information or copies received or made from copies received pursuant to the agreement, but the contractual use term does not apply to information or copies properly received or obtained from another source." [35]

7. Formation By Electronic Agents

a. Definition

"(27) 'Electronic agent' means a computer program, or electronic or other automated means, used by a person to initiate an action, or to respond to electronic messages or performances, on the person's behalf without review or action by an individual at the time of the action or response to the message or performance." [36]

b. Offer and Acceptance

"(a) A contract may be formed by the interaction of electronic agents. If the interaction results in the electronic agents' engaging in operations that under the circumstances indicate acceptance of an offer, a contract is formed, but a court may grant appropriate relief if the operations resulted from fraud, electronic mistake, or the like.

(b) A contract may be formed by the interaction of an electronic agent and an individual acting on the individual's own behalf or for another person. A contract is formed if the individual takes an action or makes a statement that the individual can refuse to take or say and that the individual has reason to know will:

(1) cause the electronic agent to perform, provide benefits, or allow the use or access that is the subject of the contract, or send instructions to do so; or

(2) indicate acceptance, regardless of other expressions or actions by the individual to which the individual has reason to know the electronic agent cannot react.

(c) The terms of a contract formed under subsection (b) are
determined under § 59.1-502.8 or § 59.1-502.9 but do not include a term provided by the individual if the individual had reason to know that the electronic agent could not react to the term." [37]

III. ENFORCING CONTRACTS

A. Traditional Principles of Jurisdiction In American Courts

1. The "Due Process" Clause of the Constitution of the United States provides that "[n]o person shall be . . . deprived of life, liberty, or property, without due process of law. . . ." [38]

2. The "Minimum Contacts" Test
   a. Before an American court can exercise personal jurisdiction over a citizen of another state or another country, due process requires that the non-resident defendant have sufficient "minimum contacts" with the forum state so that the exercise of jurisdiction would not offend "traditional notions of fair play and substantial justice." [39]
   b. To satisfy the "minimum contacts" test, three elements must be present: (1) purposeful availment; (2) relatedness; and (3) reasonableness.

3. Purposeful Availment:
   "[I]t is essential in each case that there be some act by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws." [40]

4. Relatedness and Reasonableness:
   "[S]uch contacts of the corporation with the state of the forum as make it reasonable, in the context of our federal system of government, to require the corporation to defend the particular suit which is brought there." [41]

B. Mere Advertisement or Solicitation for Sale of Goods and Services on the Internet Probably Insufficient to Establish Jurisdiction

1. In *Cybersell, Inc. v. Cybersell, Inc.* [42] the U. S. Court of Appeals for the Ninth Circuit [43] held that the defendant had not substantially availed itself of the privilege of doing business merely by posting "an essentially passive home page on the web." The mere fact that the web site could be accessed by Arizona residents was insufficient to support the inference that the defendant "deliberately directed its merchandising efforts toward Arizona residents." [44] The defendant "entered into no contracts in Arizona, made no sales in Arizona, received no telephone calls from Arizona, earned no income from Arizona, and sent no messages." [45]

2. The view of the Ninth Circuit in *Cybersell* is probably the majority view.
C. What Satisfies the "Something More" Necessary to Show "Purposeful Availment" and Therefore Jurisdiction?

1. "Interactive" Web Sites:
   
a. Zippo Mfg. Co. v. Zippo Dot Com, Inc., [52] [finding purposeful availment based on Dot Com's interactive web site and contracts with 3,000 individuals and seven Internet access providers in Pennsylvania allowing them to download the electronic messages that form the basis of the suit].

   b. Maritz Inc. v. Cybergold Inc., [53] [browsers encouraged to add address to mailing list that subscribed user to the service].

2. Evidence That Internet Activity Was Directed At, Or Bore Fruit In, Forum State:
a. Cf. *Heroes, Inc. v. Heroes Found.*, [sustained contact with District of Columbia established by, *inter alia*, web page that solicited contributions and provided toll-free telephone number *plus* defendant's use on the web page of allegedly infringing trademark and logo]; and *Pres-Kap, Inc. v. System One, Direct Access, Inc.*, [declining jurisdiction where defendant consumer subscribed to plaintiff's travel reservation system but was solicited and served instate by supplier's local representative]. [54]

b. In *EDIAS Software Int'l L.L.C. v. BASIS Int'l Ltd.*, [55] the defendant sent advertising and allegedly defamatory statements over the Internet through e-mail, its web page, and forums. The defendant had a contract with the plaintiff, an Arizona company, and made sales to plaintiff and other Arizona customers. In addition, the defendant's employees visited Arizona during the course of the business relationship with the plaintiff. The court concluded that the defendant "should not be permitted to take advantage of modern technology through an Internet Web page and forum and simultaneously escape traditional notions of jurisdiction." [56]

3. Use of an Internet Service Provider in the Forum State:

a. *CompuServe, Inc. v. Patterson*, [57] [Patterson had purposefully availed himself of the privilege of doing business in Ohio by subscribing to CompuServe, placing computer software "shareware" on CompuServe system pursuant to a Shareware Registration Agreement containing an Ohio choice-of-law clause, making sales in Ohio, and receiving transmission of funds from CompuServe in Ohio].

b. To the extent someone has engaged in "hacking" or otherwise made improper use of e-mail or an Internet web site, computer crimes statutes may provide a basis for jurisdiction and liability where it otherwise might not exist.

4. Intentional Torts

a. The Effects Doctrine

   i. In tort cases, jurisdiction may attach if the defendant's conduct is aimed at or has an effect in the forum state.

   ii. *Calder v. Jones*, [58] [National Enquirer story that libeled California resident gave rise to jurisdiction in California because California was the "focal point both of the story and of the harm suffered...[j]urisdiction...proper in California based on the "effects" of [the defendants'] Florida conduct"]

b. Does trademark infringement satisfy the "effects" test?

   i. No, according to the Ninth Circuit in *Cybersell, Inc. v. Cybersell, Inc.* [59]
ii. Five months later, on April 17, 1998, the Ninth Circuit decided *Panavision Int'l, L.P. v. Toeppen*, [60] holding that the California court had jurisdiction over an Illinois defendant accused of being a "cyber pirate," *i.e.*, someone "who steals valuable trademarks and establishes domain names on the Internet using these trademarks to sell the domain names to the rightful trademark owners." [61]

iii. In contrast to the trademark infringement at issue in *Cybersell*, in *Panavision* the Ninth Circuit found the "effects" test to be satisfied because "the present case is akin to a tort case":

"We agree that simply registering someone else's trademark as a domain name and posting a web site on the Internet is not sufficient to subject a party domiciled in one state to jurisdiction in another. As we said in *Cybersell*, there must be 'something more' to demonstrate that the defendant directed his activity toward the forum state. Here, that has been shown. Toeppen engaged in a scheme to register Panavision's trademarks as his domain names for the purpose of extorting money from Panavision. His conduct, as he knew it likely would, had the effect of injuring Panavision in California where Panavision has its principal place of business and where the movie and television industry is centered. Under the 'effects test,' the purposeful availment requirement necessary for specific, personal jurisdiction is satisfied." [62]

**D. Comparative Law**

1. The High Court of England reached a result similar to that of the Ninth Circuit in *Panavision* based on similar facts.

   a. The defendants in *British Telecomm. PLC v. One In A Million Ltd.* [63] were "domain name hijackers" who registered as domain names the names or trademarks of famous companies. For example, one of the defendants offered to sell the domain name burgerking.co.uk to the Burger King fast food chain for £25,000.

   b. The court enjoined the defendants' use of the infringing domain names and ordered them assigned to the plaintiffs.

   c. Because both the plaintiffs and the defendants were in the U.K., the issue of extraterritorial jurisdiction arose only to the extent that the defendants were required to assign certain U.S. contractual rights to domain names. In finding that the defendants were guilty of "passing
"off," the High Court found that the defendants intended to infringe the plaintiffs' trademark rights. Therefore, an exercise of extraterritorial jurisdiction would have been justified under the rationale of *Panavision*.

2. A recent decision of a French court suggests a somewhat broader view of extraterritorial jurisdiction over claims of domain name infringement than that adopted by most U.S. courts.

   a. In *Commune de Saint Tropez v. S.a. Eurovirtuel* [64] the District Court of Draguigan ordered the defendant to cease use of the Internet domain name Saint-Tropez.com in the United States.

   b. The plaintiff, the City of Saint-Tropez, is the owner of the registered French trademark SAINT-TROPEZ.

   c. The French court rejected the defendant's claim that it lacked jurisdiction on the grounds that the Saint-Tropez.com domain name was on a server in the United States. The French court rejected this argument because the web site was accessible from France.

   d. This expansive view of jurisdiction raises the potential for a "world without borders" and disputes as to whose law governs. Note, however, that the defendant was a French company. Therefore, the decision may be less remarkable than if, for example, it involved a U.S. company's domain name registration.

**E. Choice of Law and Forum Clauses**

1. "PROs"

   a. They offer the potential to avoid the application of unfavorable laws in some jurisdictions.

   b. They offer the potential to reduce litigation costs by choosing state law with which counsel is familiar, by choosing a forum which is located near the party or its counsel, or by choosing a forum which is relatively fast to decide disputes--such as the U.S. District Court for the Eastern District of Virginia [a/k/a the "Rocket Docket"].

   c. They can result in predictability of judicial interpretation [although sometimes the interpretation is predictably bad].

   d. The parties can sometimes avoid collateral litigation over what law applies.

2. "CONs"

   a. They can result in problems enforcing judgments overseas. The United States, most states and most foreign countries only will enforce foreign judgments which are final. Thus, the victorious party in its own state who must enforce its judgment in the loser's home state probably will be required to wait until all appeals have terminated before
enforcing the judgment. In addition, prevailing in litigation in the foreign forum will be useless if the loser's home state or country refuses on public policy grounds to enforce the judgment or to recognize it for res judicata purposes.

b. Vague public policy limitations, considerations of "reasonableness," and uncertainty as to the interaction of state and federal law make the enforceability of law and forum selection provisions an issue which is ripe for litigation. Of course, omitting such provisions is not necessary to avoid collateral litigation. A party can always avoid collateral litigation simply by conceding the provision's validity or waiving enforcement if the benefits afforded by the chosen law are outweighed by the costs of collateral litigation.

3. In federal courts, a forum selection provision negotiated in an arm's length negotiation by experienced businessmen is generally enforceable "absent some compelling and countervailing reason" to set it aside. [65] However, it may be unenforceable under one of two circumstances. The first recognized ground for voiding a forum selection clause is if it is so "manifestly and gravely" inconvenient that it effectively deprives the party seeking to avoid the chosen forum of a meaningful day in court. [66] The second is if enforcement would result in application of law which contravenes a strong public policy of the state in which the action is commenced. [67] Even in the case of a contract between two American parties in which a remote foreign forum is selected, the party seeking to avoid the forum selection provision on the ground of inconvenience should bear a "heavy burden" of proving that the agreement is adhesive or that the particular dispute is not covered by the agreement. [68]

4. Some states, however, have common law limitations on the enforceability of forum selection clauses. The modern view among state courts is that they will enforce forum selection provisions unless the party challenging enforcement establishes that such provisions are unfair or unreasonable, or are affected by fraud or grossly unequal bargaining power. [69] However, the law of several states is that forum selection provisions are invalid as contrary to public policy. These states include: Alabama, Arkansas, Georgia, Maine, North Carolina, Rhode Island, Texas and possibly Massachusetts and West Virginia, where there are divisions of authority. [70]

5. In federal court, federal procedural law governs federal court enforcement of forum selection provisions in diversity cases. Therefore, a potential means of circumventing state laws against forum-selection provisions is for a franchisor to file its action in federal court or remove the case to federal court.

6. The fact that a contract has a forum selection clause does not, of course, mean that the defendant will not seek a venue transfer on grounds of, for example, forum non conveniens. Mere inconvenience is not a proper ground for invalidating a forum selection provision. If inconvenience of the foreign forum was foreseeable at the time of contracting, then the party seeking to avoid a transfer into the selected forum on the ground that it is inconvenient bears the burden of showing that "trial in the contractual forum will be so gravely difficult and inconvenient that he will for all practical purposes be deprived of his day in court." [71] A First Circuit decision
applied *Bremen* to uphold a decision transferring a case from Puerto Rico, the distributor's home state, to the selected forum in Brazil, the manufacturer's home state. [72]

7. *Bremen*'s presumption in favor of enforcing forum selection provisions also applies when one party seeks to transfer venue out of the selected forum under the *forum non conveniens* doctrine and 28 U.S.C § 1404(a)(1994).

8. The Supreme Court has held that a forum selection provision in a contract is a "significant factor that figures centrally" in denying a motion to transfer venue out of the selected forum. *Stewart Org., Inc. v. Ricoh Corp.* [73] Thus, a forum selection clause must be given "controlling weight in all but the most exceptional circumstances." [74]

9. A forum selection provision, standing alone, is sufficient to confer personal jurisdiction over an out-of-state defendant. [75] Absent a statute to the contrary, choice of law provisions are enforceable in most states unless either (1) the state whose law is selected bears no reasonable relationship to the dispute or (2) the selected law contravenes a strong public policy of a state which has a materially greater interest in the dispute and would be the state whose law would apply under general conflicts rules in the absence of an effective choice of law. [76]

10. In Virginia, so long as the choice of law provision is not unconscionable, it is likely to be enforced. [77]

11. Some courts have refused to permit franchisors to use choice of law provisions to escape protectionist statutes of the franchisee's home state on the basis that enforcing the choice of law provision would contravene a strong public policy of the forum state. [78] However, many courts have also enforced choice of law clauses which circumvented protectionist laws, making the parties stick to their bargain. [79]

12. Entering into a contract containing a choice of law provision constitutes purposeful availment of the laws of the chosen state. Therefore, a choice of law provision is an important factor in establishing that federal courts in the chosen state have personal jurisdiction over an out-of-state defendant. [80] However, a choice of law clause does not by itself confer personal jurisdiction over the defendant. [81]

13. Choice of forum clauses may provide that each party consents to venue and jurisdiction in the home forum of the other party and waives all unilateral objections to the inconvenience of the forum. Mutual consent provisions allow the plaintiff before filing suit to consider whether it effectively could enforce a judgment obtained in its home state.

**F. Effect of UCITA**


   a. Enforceability:

   "(a) The parties in their agreement may choose the applicable law. However, the choice is not enforceable in a
consumer contract to the extent it would vary a rule that may not be varied by agreement under the law of Virginia.

(b) In the absence of an enforceable agreement on choice of law, the contract is governed by the law of Virginia."

b. Agreement that UCITA applies/does not apply:

"The parties may agree that this chapter, including contract-formation rules, governs the transaction, in whole or part, or that other law governs the transaction and this chapter does not apply, if a material part of the subject matter to which the agreement applies is computer information or informational rights in it that are within the scope of this chapter, or is subject matter within this chapter under § 59.1-501.3 (b), or is subject matter excluded by § 59.1-501.3 (d) (1) or § 59.1-501.3 (d) (2). However, any agreement to do so is subject to the following rules:

(1) An agreement that this chapter governs a transaction does not alter the applicability of any rule or procedure that may not be varied by agreement of the parties or that may be varied only in a manner specified by the rule or procedure, including the Virginia Consumer Protection Act of 1977 (§ 59.1-196 et seq.). In addition, in a mass-market transaction, the agreement does not alter the applicability of a law applicable to a copy of information in printed form.

(2) An agreement that this chapter does not govern a transaction:

   (A) does not alter the applicability of § 59.1-502.14 or § 59.1-508.16; and

   (B) in a mass-market transaction, does not alter the applicability under this chapter of the doctrine of unconscionability or fundamental public policy or the obligation of good faith.

(3) In a mass-market transaction, any term under this section which changes the extent to which this chapter governs the transaction must be conspicuous.

(4) A copy of a computer program contained in and sold or leased as part of goods and which is excluded from this chapter by § 59.1.501.3 (b) (1) cannot provide the basis for an agreement under this section that this chapter governs the transaction." [83]

c. Federal preemption:
(a) A provision of this chapter which is preempted by federal law is unenforceable to the extent of the preemption." [84]

d. Conflicts with public policy:

"(b) If a term of a contract violates a fundamental public policy, the court may refuse to enforce the contract, enforce the remainder of the contract without the impermissible term, or limit the application of the impermissible term so as to avoid a result contrary to public policy, in each case to the extent that the interest in enforcement is clearly outweighed by a public policy against enforcement of the term." [85]

e. Virginia Consumer Protection Act:

"(c) Except as otherwise provided in subsection (d), if this chapter or a term of a contract under this chapter conflicts with the Virginia Consumer Protection Act of 1977 (§ 59.1-196 et seq.), the Virginia Consumer Protection Act governs." [86]

f. Relationship with other laws:

"(d) If a law of this Commonwealth in effect on the effective date of this chapter applies to a transaction governed by this chapter, the following rules apply:

1. A requirement that a term, waiver, notice, or disclaimer be in a writing is satisfied by a record.

2. A requirement that a record, writing, or term be signed is satisfied by an authentication.

3. A requirement that a term be conspicuous, or the like, is satisfied by a term that is conspicuous under this chapter.

4. A requirement of consent or agreement to a term is satisfied by a manifestation of assent to the term in accordance with this chapter." [87]


"(a) The parties in their agreement may choose an exclusive judicial forum unless the choice is unreasonable and unjust.

(b) A judicial forum specified in an agreement is not exclusive unless the agreement expressly so provides." [88]
IV. THE USE OF COMPUTER CRIMES LAWS TO OBTAIN JURISDICTION

A. Advantages of Invoking Protections of Computer Crimes Laws

1. In the United States, at both the federal and state level, there are statutes enacted specifically to prohibit "hacking" and other so-called "computer crimes." Some of these statutes prohibit unauthorized access to and disclosure of communications that have been stored electronically (such as voicemail and e-mail). [89]

2. Depending upon the circumstances, such statutes may provide a more effective remedy than what is available for more traditional, "low tech" methods of trade secret misappropriation. This is so for a number of reasons, including the following:

   a. To prevail, the plaintiff whose computer system was infiltrated need not prove the existence of trade secrets. This can be a significant advantage because the fact that a "hacker" was successful makes it more difficult for the franchisor to establish the reasonableness of its security measures and that trade secret protection has not been lost.

   b. Depending upon the location of the Internet Service Provider and the web site or computer that was improperly accessed, it may be possible to establish jurisdiction in a forum that is more convenient or advantageous.

   c. Such statutes may make it easier to seal all or part of the record so that competitors, customers, and the news media do not learn of the dispute.

B. Federal Computer Crimes Legislation

1. The major federal enactments in this area include the Computer Fraud and Abuse Act of 1986, as amended by the National Information Infrastructure Protection Act of 1996.

2. The offenses under the federal statute relate to anyone who "exceeds authorized access" of a "protected computer."

   a. The term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." [90]

   b. The term "protected computer" means a computer:

      "(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not used exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

      (B) which is used in interstate or foreign commerce or
c. The term "computer" means:

"an electronic, magnetic, optical, electrochemical, or other high speed processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." [92]

d. The statutory definition of "computer" includes automated teller machines. [93]

C. U.S. Federal Electronic Communications Privacy Act

1. Federal law makes unauthorized access to stored communications a crime:

"(a) Offense. Except as provided in subsection (c) of this section whover--

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section." [94]

2. Federal law also makes unauthorized disclosure of stored communications a crime:

"(a) Prohibitions. Except as provided in subsection (b)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of
communications received by means of electronic transmission from), a subscriber or customer of such service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." [95]

3. The statute also authorizes civil actions and remedies in the form of:

   a. injunctive and declaratory relief;

   b. actual damages plus the violator's profits in an amount not less than $1,000; and

   c. reasonable attorneys' fees and litigation costs. [96]

**D. State Computer Crimes Laws**

1. Every state except Vermont has enacted computer crimes laws. Typically, these statutes provide both civil and criminal remedies against unauthorized use of a computer. [97]

2. The Virginia Computer Crimes Act, Va. Code § 18.2-152.1 et seq., is typical of enactments in this area.

   a. The offenses of the Virginia Computer Crimes Act are keyed to "use" of computers "without authority."

      i. "Use" of computers is defined as follows:

      "A person 'uses' a computer or computer network when he:

      1. Attempts to cause or causes a computer or computer network to perform or to stop performing computer operations;

      2. Attempts to cause or causes the withholding or denial of the use of a computer, computer network, computer program, computer data or computer software to another user; or

      3. Attempts to cause or causes another person to put false
ii. "Without authority" is defined as follows:

   "A person is 'without authority' when [...] he has no right or permission of the owner to use a computer or he uses a computer in a manner exceeding such right or permission...." [99]

b. The Virginia Computer Crimes Act prohibits computer fraud, [100] computer trespass, [101] computer invasion of privacy, [102] theft of computer services, [103] and personal trespass by computer. [104]

c. Persons injured by violations of the Virginia Computer Crimes Act can also recover damages, including lost profits, and the "costs of suit." [105]

3. It may be possible to prevent competitors and other from learning of the dispute.

   a. For example, the Virginia Computer Crimes Act expressly authorizes sealing the record:

      At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party. [106]

   b. Similarly, every federal court "has supervisory power over its own records and files." [107]

      i. Access to court records may be denied "where court files might . . . become a vehicle for improper purposes." [108]

      ii. Such "improper purposes" include instances where court records may be used "as sources of business information that might harm a litigant's competitive standing." [109]

E. E-Mail As Computer Crimes

1. In CompuServe v. Cyber Promotions, Inc., [110] the court held that, by sending junk e-mail to CompuServe subscribers notwithstanding requests that they stop, the defendants "have used [CompuServe's] equipment in a fashion that exceeds that consent" and that "[t]he use of personal property exceeding consent is a trespass."

2. In United States v. Kammersell, [111] the defendant was indicted for "knowingly transmit[ting] in interstate commerce to America Online, Ogden, Utah, a communication to injure the person of another by means of a bomb . . . ." Defendants moved to dismiss the indictment on the grounds that the United States
did not have jurisdiction to prosecute the matter because the email was sent from Utah to a person also in Utah and therefore was not an "interstate" communication. Because the e-mail message first went to the server's facility in Virginia and then went back to Utah, the court concluded that the defendant had used interstate commerce to transmit his message.

**F. Comparative Law**

1. The Computer Fraud and Abuse Act has served as a model for similar enactments worldwide. [112]

**G. Is Self-Help a "Computer Crime"?**

**V. REMEDIES UNDER UCITA**

**A. Available Remedies**

1. Rescission [113]
2. Cancellation [114]
3. Modification by Contract [115]
4. Liquidated Damages [116]
5. Statute of Limitations
   
   a. Four years after cause of action accrues or
   
   b. One year after breach was or should have been discovered but
   
   c. Not later than five years after cause of action accrues
   
   d. Unless limited by contract to one year (except in consumer contracts). [117]
6. Remedies for Fraud [118]
7. Compensatory Damages
   
   a. Measurement [119]
   
   b. Licensor's damages [120]
   
   c. Licensee's damages [121]
8. Recoupment [122]
9. Specific Performance [123]

**B. Special Rules for Licenses/Self-Help**

1. Licensor Remedies for Breach by Licensee
a. Complete work and identify to contract
b. Cease work
c. Relicense or dispose of
d. Other commercially reasonable steps
e. Pursue other remedies [124]

2. Licensee Remedies for Breach by Licensor
   a. Continue to use information in accordance with contract terms
   b. Pursue other remedies [125]

3. Self-Help
   a. Discontinuing access
      i. Material breach or
      ii. If agreement so provides [126]
   b. Right to possession and to prevent use [127]

4. Limitations on Electronic Self-Help
   a. Licensee must manifest assent
   b. Licensor must provide notice before disabling
   c. Licensee may recover damages for wrongful electronic self-help [128]

ENDNOTES

[*] Michael J. Lockerby is a partner in the law firm of Hunton & Williams. Hunton & Williams has more than 700 attorneys in ten American cities (Atlanta; New York; Miami; Washington, D.C.; Charlotte and Raleigh, North Carolina; Knoxville, Tennessee; and McLean, Norfolk, and Richmond, Virginia), three European cities (Warsaw, Brussels, and London), and two Asian cities (Hong Kong and Bangkok). Mr. Lockerby is resident in the firm's McLean and Richmond offices.

Mr. Lockerby's practice at Hunton & Williams includes frequent litigation of intellectual property, antitrust, tort, and contractual issues arising out of license, franchise, and distribution agreements, including in the context of electronic commerce. He regularly appears in federal courts in the Eastern District of Virginia; in other cities in which Hunton & Williams has offices (including New York and Atlanta); and elsewhere around the country. As an adjunct to his litigation practice, Mr. Lockerby negotiates, drafts, and advises clients about licensing, franchise, and distribution agreements in a number of industries. These include computer software,
telecommunications, office equipment, consumer products, motor vehicles, heavy equipment, and alcoholic beverages. He is also the author of H&W AudiTECH,® Hunton & Williams' intellectual property audit program for emerging technology companies.

Mr. Lockerby is the immediate past Chair of the Franchise and Dealership Committee of the ABA Section of Antitrust Law and current Vice Chair of the FTC Committee. On behalf of the Virginia State Bar, he has served as the Chair of the Antitrust, Franchise and Trade Regulation Section and as a member of the Board of Governors of the International Practice Section. Mr. Lockerby frequently speaks and writes about topics of interest in franchising, distribution, intellectual property, antitrust law, and the Internet. He serves on the Advisory Board of the World Internet Law Report and the World Licensing Law Review, published by BNA International in London, and on the editorial board of the ABA Franchise Law Journal. On behalf of the ABA Forum on Franchising, he has served as editor-in-chief of the Franchise Law Bibliography, published in July 1993, and of The Trade Secret Handbook for Franchise and Distribution Companies, scheduled for publication this year.

Mr. Lockerby received a B.A. in 1978 from the University of North Carolina at Chapel Hill and a J.D. in 1984 from the University of Virginia. He has previously worked for the Joint Economic Committee of the U.S. Congress and as a legislative assistant for the late U.S. Senator John Heinz (R - Pennsylvania).

[1.] 104 F.3d 670, 671 (4th Cir. 1997).
[2.] Based in Richmond, Virginia, the U.S. Court of Appeals for the Fourth Circuit has appellate jurisdiction over the U.S. District Courts in Maryland, Virginia, West Virginia, North Carolina, and South Carolina.
[4.] FED. R. CIV. P. 34(a) (emphasis applied).
[6.] 995 F.2d 1376, 1383 (7th Cir. 1993).
[7.] Based in Chicago, Illinois, the U.S. Court of Appeals for the Seventh Circuit has appellate jurisdiction over the U.S. District Courts in Illinois, Indiana, and Wisconsin.
Based in Cincinnati, Ohio, the U.S. Court of Appeals for the Sixth Circuit has appellate jurisdiction over the U.S. District Courts in Kentucky, Michigan, Ohio, and Tennessee.

*Compuserve*, 89 F.3d at 1260-61.


Id. § 2B-113.


The term "electronic record" is defined as "a record created, stored, generated, received, or communicated by electronic means." UETA. § 102(7) (Draft Mar. 23, 1998) (subsequently amended 1999). The term "record" is defined as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium, and is retrievable in perceivable form." UETA. § 102(16) (Draft Mar. 23, 1998).

Id. § 201(a)-(b).

The term "signature" is defined as "any symbol, sound, process or encryption of a record in whole or in part, executed or adopted by a person or the person's electronic agent with intent to: (A) identify that person; (B) adopt or accept a term or a record; or (C) establish the informational integrity of a record or term that contains the signature or to which a record containing the signature refers." UETA § 102(20) (Draft Mar. 23, 1998). UETA defines "sign" as "to execute or adopt a signature." Id. § 102(19). An "electronic signature" is defined as "any signature in electronic form, attached to or logically associated with an electronic record." Id. § 102(8).


UTAH CODE ANN. §§ 46-3-401, 403 (1998).

Id. §46-3-401.


Id. § 59.1-501.2(6).

Id. § 59.1-501.12(a)-(d).

Id. § 59.1-501.5(d).

Id. § 59.1-501.7.
Based in San Francisco, California, the U.S. Court of Appeals for the Ninth Circuit has appellate jurisdiction over the U.S. District Courts in Alaska, Arizona, California, Idaho, Montana, Nevada, Oregon, Washington, Guam, and Hawaii.

"Cybersell FL's web page simply was not aimed intentionally at
Arizona knowing that harm was likely to be caused there to Cybersell AZ.

[60.] 141 F.3d 1316, 1318 (9th Cir. 1998).

[61.] Id.

[62.] Id. at 1322 (citing Cybersell, 130 F.3d at 418).


[66.] Id. at 19.

[67.] Id. at 15.

[68.] Id. at 17.


[72.] Royal Bed & Spring Co. v. Famossul Industria E Comercio de Moveis Ltda., 906 F.2d 45 (1st Cir. 1990) (diversity case).


[74.] Id. at 33 (Kennedy, J. concurring); In re Ricoh Corp., 870 F.2d 570 (1989).


[80.] Burger King Corp. v. Rudzewicz, 471 U.S. 462, 482 (1985).

[81.] Id. at 478.

[83.] Id. § 59.1-501.4.

[84.] Id. § 59.1-501.5.

[85.] Id. § 59.1-501.5.

[86.] Id.


[88.] Id. § 59.1-501.10.


[91.] Id. § 1030(e)(2).

[92.] Id. § 1030(e)(1).

[93.] United States v. Sykes, 4 F.3d 697, 698 (8th Cir. 1993).


[95.] Id. § 2702.

[96.] Id. § 2707.


[98.] VA. CODE ANN. § 18.2-152.2(4) (emphasis added) (Michie Supp. 2000). See generally VA CODE ANN. § 18.2-152.2 (providing definitions).

[99.] Id. (emphasis added).

[100.] "Computer fraud" is defined as "use" of a computer or computer network "without authority" and with the intent to "(o)btain property or services by false pretenses;" "(e)mbezzle or commit larceny;" or "(c)onvert the property of another." VA. CODE ANN. § 18.2-152.3.

[101.] "Computer trespass" is defined as "use" of a computer or computer network "without authority" and with the intent to:

"1. Temporarily or permanently remove computer data, computer programs, or computer software from a computer or computer network;

"2. Cause a computer to malfunction regardless of how long the malfunction persists;

"3. Alter or erase any computer data, computer programs, or computer software;

"4. Effect the creation or alteration of a financial instrument or of an electronic transfer of funds;
5. Cause physical injury to the property of another; or

6. Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.

VA. CODE ANN. § 18.2-152.4.

[102.] "Computer invasion of privacy" is defined as "use" of a computer or computer network and intentional examination "without authority" of "employment, salary, credit or any other financial or personal information relating to any other person." VA. CODE ANN. § 18.2-152.5(A).

[103.] "Theft of computer services" is defined as "use" of a computer or computer network" with intent to obtain computer services without authority." VA. CODE ANN. § 18.2-152.6.

[104.] "Personal trespass by computer" is defined as "use" of a computer or computer network without authority and with the intent to cause physical injury to an individual." VA. CODE ANN. § 18.2-152.7.

[105.] Id. § 18.2-152.12.

[106.] VA. CODE ANN. § 18.2-152.12(D) (emphasis supplied).


[108.] Id. at 598 (emphasis supplied).

[109.] Id. at 598.


[114.] Id. § 59.1-508.2.

[115.] Id. § 59.1-508.3.

[116.] Id. § 59.1-508.4.

[117.] Id. § 59.1-508.5.


[119.] Id. § 59.1-508.7.
Id. § 59.1-508.8.

Id. § 59.1-508.9.

Id. § 59.1-508.10.


Id. § 59.1-508.12.

Id. § 59.1-508.13.

Id. § 59.1-508.14.

Id. § 59.1-508.15.