

**THE UNIFORM COMPUTER INFORMATION
TRANSACTIONS ACT (UCITA) AND REVERSE ENGINEERING —
RESTRIKING THE BALANCE**

By:

**Proprietary Rights Committee
Computer Law Section
State Bar of Michigan**

Chairman

**David R. Syrowik
Brooks & Kushman P.C.
Southfield, Michigan**

Committee Members

**Mitchell A. Goodkin
William M. Hanlon, Jr.
Mary I. Hiniker
John S. LeRoy
Ronald M. Nabozny
Paul J. Raine**

***State Bar of Michigan
67th Annual Meeting
September 27, 2002
Grand Rapids, Michigan***

I. INTRODUCTION

The Uniform Computer Information Transactions Act (“UCITA”) is a proposed uniform state law governing transactions involving “computer information” (such as the licensing of computer software or databases) that was promulgated in the summer of 1999 by the National Conference of Commissioners of Uniform State Laws (“NCCUSL”). In other words, UCITA is an enactment similar to Article 2 of the Uniform Commercial Code (“UCC”). However, whereas Article 2 governs sales of goods, UCITA applies to licenses of computer software and other computer information transactions.¹

On January 31, 2002, a special UCITA Working Group established by the American Bar Association issued a report. Among the specific areas of concern was “clarity and ease of use” of UCITA. The January Report stated that:

The Working Group’s principal concern with UCITA, as presently drafted, is that it is extremely difficult to understand. One underlying reason for this is that computer information transactions impact on several areas of the law, such as intellectual property law²

One of the major criticisms of UCITA, from an intellectual property point of view, is its potential use to eliminate or severely reduce “reverse engineering,” which many feel is permitted for computer programs under certain circumstances under both Federal and state law.

On May 29, 2002, the Standby Committee for UCITA approved 38 recommended amendments³ addressing, in whole or in part, 10 of 11 concerns raised by the ABA Working Group, in its own report to the ABA Board of Governors. Recommended Amendment #6 called for a new Section 118, entitled “Terms on Reverse Engineering.” New Section 118 seeks to answer some of the critics of UCITA. The recommended amendments, including new Section 118, were considered and approved by the NCCUSL commissioners at their 2002 Annual Meeting in August by a vote of 49 to 0.

After providing an overview of some of the intellectual property aspects of UCITA and reverse engineering, this report reviews the law of reverse engineering and then compares and contrasts new Section 118 with the reverse engineering provisions of the European Community (EC) Directive on the Legal Protection of Computer Programs⁴ to which new Section 118 has been compared by the Standby Committee.

II. BACKGROUND

A. UCITA and its Relation to Intellectual Property Law

1. The NCCUSL View

In 2000, the NCCUSL prepared a summary of UCITA.⁵ A copy of the summary is reproduced in its entirety in Appendix A. In that summary, the NCCUSL put forth its view of how UCITA interacts with established intellectual property law.

As noted in the Summary, UCITA gives courts the power and responsibility to reconcile commercial licensing law with intellectual property law, most of which is federal in origin. More specifically, Section 105(a) of UCITA permits federal law preemption, while Section 105(b) permits public policy invalidation as follows:

- (a) A provision of this [Act] which is preempted by federal law is unenforceable to the extent of the preemption.
- (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.

The general reporter's comments to Section 105 on one hand state that "Balancing the rights of owners of information against the claims of those who want access is complex and has been the subject of considerable controversy and negotiation at both the federal level and

internationally.” On the other hand, the reporter’s comments state that “Subsections (a) and (b) strike the balance between fundamental interests in contract freedom and fundamental public policies such as those regarding innovation, competition, and free expression. The use of these general principles will enable the courts to react to changing practices and technology; more specific prohibitions would lack flexibility and would inevitably fail to cover all relevant contingencies.”

The reporter’s comments to the Section 105(a) preemption provision states that “Except for rules that directly regulate specific contract terms, no general preemption of contracting arises under copyright or patent law. See, *National Car Rental System, Inc. v. Computer Associates Int’l, Inc.*, 991 F.2d 426 (8th Cir. 1993); *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996). Case law will continue to develop in this area. As state law, this Act does not define whether or when federal preemption may occur.”⁶

Of interest is the citation of the *ProCD* case, where federal preemption was not found in a shrinkwrap license transaction involving software.⁷ Many courts and commentators that have considered the issue have concluded that such transactions are sales of goods and are covered by Article 2 of the UCC.⁸

The reporter’s comments to Section 105(b) explicitly discuss reverse engineering of computer programs:

In part because of the transformations caused by digital information, many areas of public information policy are in flux and subject to extensive debate. In several instances, these debates are conducted within the domain of copyright or patent laws, such as whether copying a copyrighted work for purposes of reverse engineering is an infringement.

This Act does not address these issues of national policy, but how they are resolved may be instructive to courts in applying this subsection. A recent national statement of policy on the relationship between reverse engineering, security testing, and copyright in digital information can be found at 17 U.S.C. § 1201 (1999). It expressly addresses reverse engineering . . . in

connection with circumvention of technological protection measures that limit access to copyrighted works. It recognizes a policy to not prohibit some reverse engineering where it is needed to obtain interoperability of computer programs. . . . This policy may outweigh a contract term to the contrary.

17 U.S.C. § 1201 was the subject of last year's report⁹ by the Proprietary Rights Committee of the Computer Law Section of the State Bar of Michigan which stated the following with respect to the issue of reverse engineering and the Digital Millennium Copyright Act which created an entirely new cause of action against people who circumvent "copy protection" schemes or make devices that enable others to do so:

Section 1201(f) creates a narrowly limited "reverse engineering" exemption for the circumvention of technological measures controlling access to a computer program. The Section 1201(f) exemption applies to the reverse engineering of copyrighted computer programs for the sole purpose of identifying and analyzing those elements of the protected work "necessary to achieve interoperability" with other independently created programs, and that have not previously been readily available to the person engaging in the circumvention. For purposes of Section 1201(f), "interoperability" is defined as the ability of computer programs to exchange and share information.

2. The Opposing View

UCITA has remained quite controversial, especially Section 209 of UCITA, which validates mass-market licenses for computer information such as computer programs. Such controversy arises, at least in part, because in a typical mass-market software transaction, there is no bargaining over license terms. The purchaser (licensee) commonly obtains a single copy of the software, along with documentation, in a box at a retail software store. The box contains a single price, which the purchaser pays up front and which constitutes the entire payment for the "license." The purchaser pays sales tax on the "license." The license does not run for a definite term and need not be renewed, but it is perpetual unless terminated by the vendor (something that almost never occurs). Consequently, in light of these indicia, most purchasers think they are *buying* a physical copy of a program.

In a letter dated July 9, 1999, reproduced in its entirety in Appendix B, the Federal Trade Commission (*i.e.*, “FTC”) attacked UCITA. As noted in the letter, one of the principal prongs of its attack on the Act was its attack on Section 105 of UCITA. In particular, the FTC stated that even if a court concludes that reverse engineering is a “fundamental public policy,” it still must balance that policy against the policy favoring enforcement of contracts.

UCITA Section 105(b) directs courts to refuse to enforce a term only “to the extent that the interest in enforcement is *clearly outweighed* by a public policy against enforcement of the term.” (Emphasis supplied.) “Clearly outweighed” is an obviously high standard to meet. The reporter’s comment states that reverse engineering “*may* outweigh a contract term to the contrary,” but does not state that reverse engineering *clearly* outweighs a term to the contrary. This uncertainty “could upset the delicate balance between intellectual property and competition policy, which has been carefully calibrated”

The issue of reverse engineering rights is also part of a more general issue.

Advocates for UCITA argue that UCITA is modeled very closely and directly on the very successful UCC Article 2, and that UCITA will do nothing more than provide the needed consistency for transactions involving computer information across the states that is provided by the UCC for other contracts.

Opponents argue that UCITA generally does not provide the necessary consumer protections. They point out that during the many years that UCC Article 2 has been in effect in the states, extensive consumer protection statutes and case law has been needed and developed in relation to the various versions of UCC Article 2 that the states have adopted. If UCITA is adopted without additional protections specific to UCITA being concurrently adopted, consumers will not have the protections for the subject matter of UCITA that have been established with regard to the UCC.

B. Reverse Engineering

In general, “reverse engineering” is:

A method of obtaining technical information by starting with a publicly available product and determining what it is made of, what makes it work, or how it was produced. The engineering effort goes in the reverse direction of usual engineering efforts, which start with technical data and use it to produce a product. Reverse engineering starts with the product and uses it to determine the technical data and know-how that was used to make the product.¹⁰

The resulting technical information which is obtained by reverse engineering is often used to make a similar product at a substantially reduced investment of money and human resources.

Reverse engineering has been authoritatively defined by the Supreme Court as “[T]he process of starting with the known product and working backwards to divine the process which aided in its development or manufacture.”¹¹

In the case of most copyrightable works, once the author has consented to publication, the ideas and other unprotected material contained therein may be readily examined and put to further use. The situation with respect to computer programs is quite different. Software products are typically distributed in object code form only, a fact that makes it difficult to discover the ideas and principles contained in a program without reverse engineering. If reverse engineering is completely forbidden, software developers could use copyright law to get de facto monopolies on functional process and systems embodied in programs that may not have met patent standards.¹²

Consequently, in order to examine and use the ideas and other unprotected material contained in a computer program, the computer program must be reverse engineered such as by “disassembly” or “decompilation.” While the terms “reverse engineering” and “decompilation” are occasionally used interchangeably, such usage is inaccurate. “Reverse engineering” encompasses any method of studying a computer program’s function, and may include studying published documentary material, running the program or conducting tests on the program without making a copy, as well as making copies of all or parts of the program whether through decompilation or not.

“Decompilation” and “disassembly” are narrower terms, referring to the reverse compiling or reverse assembly, respectively, of computer programs to create a pseudo-source code version of the program which is then analyzed to determine the structure and logic of the

original. The knowledge gained through reverse engineering may be used for a variety of purposes (*e.g.*, to develop similar software, or even hardware).

III. THE LAW OF REVERSE ENGINEERING

A. *In General*

The United States Supreme Court has emphasized that trade secret law does not restrict the use of information acquired through independent discovery or reverse engineering of products fairly and honestly acquired such as by the purchase of product on the open market.¹³

The Uniform Trade Secrets Act, which the state of Michigan recently enacted at MCLA § 445.1901 *et seq.*, expressly provides that reverse engineering a commercially available product is a legitimate means of discovering a trade secret. Commissioners' Comment to Section 1 of the Act provides:

Proper means include: . . .

2. Discovery by 'reverse engineering,' that is, by starting with the known product and working backward to find the method by which it was developed. The acquisition of the known product must, of course, also be by a fair and honest means, such as purchase of the item on the open market for reverse engineering to be lawful

Furthermore, the Restatement (Third) of Unfair Competition states at § 43 that "independent discovery and analysis of publicly available products or information are not improper means of acquisition."¹⁴

As stated in the Comment to § 43 of the Restatement,

Unless a trade secret has been acquired under circumstances giving rise to a duty of confidence, a person who obtains the trade secret by proper means is free to use or disclose the information without liability. Unlike the holder of a patent, the owner of a trade secret has no claim against another who independently discovers the secret. Similarly, others remain free to analyze products publicly marketed by the trade secret owner and, absent protection under a patent or copyright, to exploit any information acquired through such “reverse engineering.” A person may also acquire a trade secret through an analysis of published materials or through observation of objects or events that are in public view or otherwise accessible by proper means.¹⁵

A “duty of confidence” can arise through contract such as a license agreement having a confidentiality provision¹⁶ which may be provided by UCITA without negotiation in a mass-market situation.

In summary, in the absence of protection under a patent, copyright or duty of confidence, and assuming that the product or other material that is the subject of the reverse engineering was properly obtained, the process of reverse engineering is not infringement of any trade secrets in the data embodied in a product and is legitimate and legal competitive behavior.

B. As it Relates to Computer Programs

The leading case involving the reverse engineering of computer programs in the U.S. is the *Sega* case.¹⁷ The *Sega* Case involved disassembly and decompilation in order to get information necessary to make games compatible with plaintiff’s game system, the court held that it was a fair use of a copyrighted computer program for a competitor to disassemble the program and make an intermediate copy solely in order to determine the uncopyrightable concepts embodied in the program. “We conclude that where disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program

and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law.

The court reviewed each of the four fair use factors under 17 U.S.C. § 107. As to the first factor, although defendant's broad purpose was commercial, the fact that its direct copying was only for an intermediate stage, and therefore any resulting commercial exploitation was only indirect, overcame the rebuttable presumption that commercial uses are unfair. In fact, the narrow purpose for which defendant undertook the disassembly was to study the functional requirements in plaintiff's code, so that it could produce its own games compatible with plaintiff's console.

Decisive to the second factor was the fact that defendant had no viable alternative to its reverse engineering; "disassembly was necessary in order to discover the functional specifications" for a game compatible with plaintiff's product.

As to the third factor, although defendant did disassemble plaintiff's entire copyrighted work, "where the ultimate (as opposed to direct) use is limited" as on the facts presented, the court held it to be of very little weight.

Turning to the fourth factor, market impact, the direct use of the copied material was to study the functional requirements for compatibility; although plaintiff might lose some sales from defendant's competition, there was not direct competition between the parties.

A subsequent case has extended the holdings of the *Sega* case. Defendant *Connectix*, seeking to learn how to inter-operate with Sony's video game software, repeatedly disassembled the BIOS software and also adapted the software to operate in a different environment where its features could be more closely observed.¹⁸ The court ruled fair as a matter of law the intermediate copying that took place for purpose of reverse engineering in order to manufacture competing hardware for the following reasons:

- ☐ Because *Sony* did not make information about its BIOS publicly available, *Connectix* needed to engage in reverse engineering to access its functional elements (*i.e.*, second factor);
- ☐ Intermediate copying was “necessary” to accomplish that task (*i.e.*, first factor);
- ☐ Such copying did not cease being “necessary” even though iterated repeatedly in an emulated environment (*i.e.*, third factor);
- ☐ Most critically, the financial loss to *Sony* accrued not to its copyrighted works, but to the hardware used to access those works – “Sony understandably seeks control over the market for devices that play games Sony produces or licenses. The copyright law, however, does not confer such a monopoly (*i.e.*, fourth factor).

Taken together, the *Sega/Sony* cases don’t appear to limit the method or quantity of intermediate copying (*i.e.*, decompilation) of a computer program. Rather, the focus of the courts’ inquiry was primarily directed to the ultimate objects or purposes for which the reverse engineering was done. In other words, the courts are primarily concerned with the effects on the market for the original computer program. Such reverse engineering is allowed if done for a legitimate reason.

IV. NEW SECTION 118 OF UCITA AND THE EUROPEAN COMMUNITY’S SOFTWARE DIRECTIVE

The Standby Committee’s comment on Section 115, a predecessor of New Section 118 of UCITA, explains that “[i]t adopts the position taken in Europe, which permits reverse engineering despite a contrary contract clause if the reverse engineering is needed for interoperability and is permitted under trade secret, copyright, and other law.”

Consequently, in order to understand New Section 118, it is important to understand “the position taken in Europe.”

A. *The Software Directive*

On May 14, 1991, the European Community (EC) adapted its Directive on the Legal Protection of Computer Programs.¹⁹ A copy of Articles 5, 6 and 9 of The Directive is attached hereto as Appendix C, since it is these articles which are relevant to the issue of reverse engineering of computer programs.

In general, the Directive strictly limits not only when reverse engineering will be tolerated, but also how the information obtained by reverse engineering can be utilized.

1. *Reverse Engineering Other Than Decompilation*

Initially, Article 5(3) states that one must have “a right to use a copy of a computer program” one intends to analyze. This should present no barrier to legitimate developers, since it requires merely that one not use a pirated copy of the program. In this process, the engineer does not take the software apart to see how it works. Rather, the engineer tests the software by feeding it instructions or commands to see how it works.

Second, Article 5(3) permits the software engineer to “observe, study, or test the functioning of the program. This is what an engineer does when conducting “black box” analysis. Other types of “reverse analysis” include test runs, memory dumps, and the like. For example, when performing line traces, the engineer transmits messages from the analyzed program to another program or device and uses a device called a line tracer to determine how the programs interact.

Third, Article 5(3) allows the software engineer to determine the “ideas and principles” underlying any element of the computer program. This includes determining interface specifications, which, being the rules and methods by which a program interacts with other products, constitute “ideas and principles.”

Fourth, Article 5(3) permits the software engineer to observe study, or test the functioning of the program while “loading, displaying, running, transmitting or storing” the program. While the particular acts involved should be determined in each individual case, it seems that all the forms of analysis at issue here would be conducted while performing one or more of the acts listed in Article 5(3).

Finally, Article 5(3) provides that for the analysis to be allowable, one must be “entitled to do” the underlying operations involved. This provision is simply intended to guard against use of this article illegitimately to expand permitted uses of a program.

2. Reverse Engineering Through Decompilation

Articles 4(a) and (b), referred to in Article 6.1, give, respectively, the author of the computer program (1) the exclusive right to do or to authorize the permanent or temporary reproduction of the work, including loading, displaying, running, transmission, or storage of the program to the extent such acts necessitate reproduction, and (2) the right to translate, adapt, arrange or alter the program. These rights are limited by Article 6.

The introductory paragraph of Article 6 is critical since it sets forth the permissible purpose for decompilation. Decompilation may be performed only if it is “indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other computer programs.”

Article 6.1(b) states that decompilation may be conducted only “as a last resort” if the needed information is not readily available.

Article 6.1(c) states that decompilation is limited to those parts of the code that are necessary to achieve interoperability.

Article 6.2(a) states that the information obtained through decompilation may not be used for purposes other than interoperability including, under Article 6.2(b), giving it to others who do not use it to achieve interoperability, and under Article 6.2(c), is not used for the development, production, or marketing of a computer program that is substantially similar to the original, or for any other act that infringes copyright.

Article 6.3 states that decompilation may not unreasonably prejudice the author's legitimate interests or conflict with the author's exploitation of the work (*i.e.*, the effect of the use upon the market for the work).

Under Article 6.1(a), decompilation may only be carried out by a purchaser of the program, a licensee, or another person having a right or authorization to use the program.

It is important to note that Article 6 permits decompilation to achieve interoperability "with other programs." Consequently, a compatible program created using information desired through decompilation may compete with the decompiled program insofar as it interoperates with other programs in the same way that the decompiled program does.

Also, one may not decompile a computer program solely to research its underlying ideas unrelated to interoperability. It is also important to note that under Article 9(1), the exceptions provided in Article 5(3) and Article 6 cannot be overridden by contract.

B. New Section 118

New Section 118 is as follows:

SUBPART J. REVERSE ENGINEERING

SECTION 118. TERMS ON REVERSE ENGINEERING

(a) In this section, “interoperability” means the ability of computer programs to exchange information and of such programs mutually to use the information that has been exchanged.

(b) Notwithstanding the terms of a contract subject to this Act, a licensee that lawfully obtained the right to use a copy of a computer program may identify, analyze, and use those elements of the program necessary to achieve interoperability of an independently created computer program with other programs including adapting or modifying the licensee’s computer program, if:

- (1) the elements have not previously been readily available to the licensee;
- (2) the identification, analysis, or use is performed solely for the purpose of enabling such interoperability; and
- (3) the identification, analysis or use is not prohibited by law other than this Act;

(c) As applicable, identification, analysis, or use of elements of a computer program for a purpose other than described in this section is governed by Section 105(b).²⁰

The above language provides a right to reverse engineer very analogous to the Software Directive of the European Community.

Paragraph (b) is critical since it sets forth the permissible purpose for reverse engineering. Reverse engineering may be performed only if it is “necessary to achieve interoperability of an independently created computer program with other programs.”

Paragraph (b)(1) states that reverse engineering may be conducted only if the elements of the program to be reverse engineered were not readily available.

Paragraph (b) also states that reverse engineering is limited to those elements of the program that are necessary to achieve interoperability.

Paragraph (b)(2) states that the information obtained through reverse engineering may not be used for purposes other than interoperability.

Paragraph (b)(3) states that reverse engineering is permitted unless prohibited by another law.

Paragraph (c) states that reverse engineering done for any other reason is governed by § 105(b) of UCITA. An example may be where the reverse engineering is done to a computer program to research its underlying ideas unrelated to interoperability.

Under Paragraph (b) it appears that reverse engineering may only be carried out by a licensee who has a right or authorization to use a copy of the program.

V. CONCLUSION

Reverse engineering of a computer program by decompilation, to the extent that it involves making copies or adaptations of the program, implicates copyright rights. Whether those copies are infringing will generally depend on whether they can be considered “fair use” under § 107 of the copyright statute.

New Section 118 of UCITA establishes a “bright line” test or “safe harbor” that software developers can follow in the course of reverse engineering the computer programs of others. While not a particularly broad exception, it does restrike the balance between software developers and should promote some measure of “interoperability” and competition in the software industry.

Software developers may still be able to rely on § 107 and the case law on fair use and reverse engineering with respect to competitive computer programs, since contractual provisions prohibiting fair use may be preempted by § 301 of the Copyright Act. However,

recent case law suggests that prohibitions against reverse engineering, even in shrinkwrap licenses, are not preempted by the Copyright Act.

APPENDIX A

SUMMARY OF THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT

The National Conference of Commissioners on Uniform State Laws promulgated the Uniform Computer Information Transactions Act (UCITA) in 1999. This act provides a comprehensive set of rules for licensing computer information, whether computer software or other clearly identified forms of computer information. Computerized databases and computerized music are other examples of computer information that would be subject to UCITA. It would also govern access contracts to sites containing computer information, whether on or off the Internet. UCITA would also apply to storage devices, such as disks and CD's that exist only to hold computer information. Other kinds of goods which contain computer information as a material part of the subject matter of a transaction may also be made subject to UCITA by express reference in a contract. Otherwise, other law would apply, such as the law of sales or leases for most transactions. UCITA would not govern contracts, even though they may be licensing contracts, for the traditional distribution of movies, books, periodicals, newspapers, or the like.

For the most part, the rules governing computer information contracts in UCITA are default rules. This means that they may be waived or varied by contract, and that in almost all cases the terms of a contract will prevail over a contrary rule in UCITA. Rules generally relating to fairness of the contract process are not default rules, and cannot be disclaimed by contract. Included in the rules that may not be disclaimed are the obligation of good faith, diligence, and reasonableness; limitations on enforcement imposed by unconscionability and fundamental public policy; and any standard of care prescribed in UCITA. Express rules for consumers, also, may not generally be disclaimed.

UCITA's rules govern licensing of contracts for computer information from formation through performance, including remedies if there is a breach of contract. Included in UCITA are rules for warranties, both implied and express, and rules pertaining to risk of loss in a computer information transaction. Most of the rules in UCITA are the traditional and familiar rules of contract from the law of sales and from the common law, but adapted to the special nature of computer information licensing contracts. Freedom of contract is a dominating underlying policy for UCITA, exactly as that principle is the foundation for the law of commercial transactions, generally, and exactly as that law has served all commercial transactions in the United States and has contributed to the economic growth and health of the United States.

A licensing contract involves transferring computer information such as software or other computerized information, from vendor (called licensor) to recipient (called licensee). A license grants informational rights to the licensee. Informational rights include any intellectual property rights derived from copyright, patents and the like, but also all other rights in information that any other law provides to a person that allows control of the information or

restriction on the use of the information by other persons. The difference between a licensing contract and a sale contract is that the license generally contains restrictions on use and transfer of the computer information by the licensee during the life of the contract, and it may or may not transfer title to the licensee. A breach of express restrictions on use and transfer in the contract provides a remedy to the licensor.

A license under UCITA is not fundamentally rooted in intellectual property law such as patent or copyright law. A license under UCITA is simply a commercial contract, dependent wholly on the parties' ability to enter into a normal, commercial contract, just as a contract of sale or lease is simply and wholly a commercial contract. However, intellectual property rights may be licensed in a contract subject to UCITA. UCITA may not be used to vary or extend informational rights that are intellectual property rights, and expressly recognizes preemption by copyright, patent, or other federal intellectual property law in Section 105(b).

Like the law of sales and leases, in general, the right to contract is constrained by principles of unconscionability, good faith and fair dealing, UCITA has an additional restraint, an express power for a court to deny enforcement of a provision in a licensing contract that violates fundamental public policy. This public policy defense is unique in UCITA. An essential purpose of this defense is to give courts some latitude in reconciling commercial licensing law with the principles of intellectual property law. Most intellectual property law is federal, and UCITA expressly recognizes the preemptive effect of that federal law. But the public policy defense gives courts an additional power to consider intellectual property principles purely within the context commercial law.

Why is there a need for licensing contracts, rather than sale contracts for computer information? Computer information is peculiarly vulnerable to dissipation of its value by copying. The genius of computers is their ability to retain and copy information. Copies of information look just like their originals. In fact, everything is a copy. There are no true originals. Copies can be duplicated in huge numbers and disseminated to millions of users in times measured in less than seconds. Therefore, those who invest capital, intellectual effort and labor into the creation of valuable computer information may lose the economic value of their products in seconds. Without the ability to control copying and dissemination of computer information, vendors risk losing everything. The risk is so great that without licensing, the development of computer information products could become uneconomical and the great economic benefit of computer information products could be lost.

The term "copy" is, in fact, defined in UCITA as the "medium on which information is fixed on a temporary or permanent basis and from which it can be perceived, reproduced, used, or communicated, either directly or with the aid of a machine or device." Transfer of a copy is the basis of a licensing transaction. UCITA clearly separates transfer of a copy from transfer of ownership of informational rights. Title of a copy is separate from title to the informational rights, and may be transferred separately. A licensee's rights are not dependent upon transfer of title to the informational rights, although a license contract may expressly transfer title to informational rights and/or title to a copy. Transfers under UCITA are basically

transfers of copies. The basic restrictions in licensing contracts are usually restrictions on creating further copies.

Licensing of information is the standard of the computer information business today. The huge bulk of vendors license their computer information products. UCITA, therefore, does not originate licensing contracts. UCITA was developed to provide basic, recognizable default rules for the existing licensing activity that goes on and expands as commerce in computer information expands. That expansion is the primary source of economic development in the United States and is projected to be the economic mainstay of the United States for the foreseeable future. UCITA, therefore, is responding to existing economic activity and a mode of contract upon which the computer information industry, itself, has come to rely. Firming the law and establishing some certainty with respect to the rules that apply, and that apply uniformly, is the modest goal of UCITA. It is not a radical, destabilizing proposal. It is familiar law adapted to ongoing economic activity that can use stable, predictable law that otherwise does not now exist.

These are some highlights of UCITA:

Mass market license. Traditionally, contract formation contemplates some negotiation and arms-length give and take between contracting parties. Commercial contract law has long since abandoned this image of contracting activity as the only image. Article 2 of the Uniform Commercial Code has long had rules governing contracts that do not form in the traditional image, and has legitimized form contracts for sales of goods for nearly half-a-century. The mass-market license is an electronic form contract for computer information licensing, exactly as there have been form contracts for the sales of goods for a very long time. The difference is that a mass-market license is often presented with the package for the computer information found in retail stores, and, more importantly as electronic commerce grows, as part of the transfer of computer information, electronically, from computer to computer. Whether called "shrink-wrap" or "click-wrap," these are mass-market licenses. UCITA treats mass-market licenses differently from negotiated licenses. A mass-market license is not enforceable against the licensee unless the terms to be enforced are readily available to the licensee and until the licensee has had an appropriate time to review them. If, upon review, the licensee does not like the license contract or any part of it, the copy of the computer information may be returned to the vendor for a refund, plus reasonable expenses for making a rightful return and compensation for damages to a processing system by the removal of the information from that system. This right of return may not be waived or disclaimed in a contract. Nowhere else in the commercial law is there such a no-fault return policy for rejecting or repudiating a contract.

Warranties of license are incorporated into UCITA, based on the warranty provisions for sale of goods under Article 2 of the Uniform Commercial Code. But computer information requires special implied

warranties. One is the warranty of compatibility of computer systems under Section 405(b). The licensor has an implied warranty, if the licensee is relying upon the licensor for skill and judgment in selecting components of a computer system, that the components will function together as a system.

Implied warranties may be disclaimed. Disclaimers in mass-market contracts must be conspicuous. Any affirmation of fact or promise made by a licensor as part of the basis of the bargain, becomes an express warranty of the licensor.

There are special rules for communication of computer information in electronic form. Since these transactions are almost all electronic, and faceless, it is necessary to have rules governing the attribution of electronic signatures, and the accuracy of electronic messages. Part 2, Subpart B is largely devoted to these communications rules. The term "authenticate" is the basis for these rules. A signature or its electronic equivalent is the basic means of authentication under UCITA. That "authentication" is attributed to the person whose intentional act that "authentication" is. A party relying upon that authentication has the burden of establishing attribution, which may be shown in any manner, including evidence of the efficacy of any "attribution procedure" used in the communication. An "attribution procedure" is any procedure that provides greater assurance than a simple transmission of information that the "authentication" is that of the party to which it is attributed. There are both simple and complex attribution procedures available for identifying the person who sends an electronic communication, and persons may choose the procedures that suit their particular transactions.

Attribution procedures may have impact on message content in an electronic communication. If a procedure is in place to detect errors or changes in the message communicated, a party that conforms to the procedure is not bound by an error or change that results because the other party does not conform to the procedure. There is a special rule for consumers. Consumers who make errors while entering automated transactions are not bound by the unintended erroneous message, so long as the consumer notifies the other party of the error promptly after it is identified, properly returns the computer information received and has not obtained value or benefit from using the information.

An "access contract" is a contract to enter the information system (read computer) of another to obtain information, or use that information system for specific purposes. Most current computer users have access contracts, if for no other reason than to use the Internet. UCITA governs these contracts with special rules relating to rights of access in Section 611.

UCITA also governs support contracts, and service contracts for the correction of performance problems. No licensor of information is required to provide such contracts (computer software support services are common), but if it does, it is subject to the express terms of the contract, or if silent, to what is "reasonable in light of ordinary standards of the business, trade, or industry...."

In Section 816, UCITA allows a licensor to disable computer information subject to a license and in use by a licensee for breach of contract. There are substantial limitations upon the exercise of this remedy. The remedy is not available unless the licensee has manifested assent to the specific part of the licensing contract that permits exercise of the remedy. There must be notice to the licensee at least 15 days prior to the exercise of the remedy. This notice gives the licensee the opportunity to cure the breach. The licensor may not exercise the remedy if it knows that exercise "will result in substantial injury or harm to the public health or safety or grave harm to the public interest substantially affecting third parties not involved in the dispute" (between licensor and licensee). The conditions for exercise of the remedy in Section 816 may not be waived or varied by contract.

These are some of the provisions in the Uniform Computer Information Transactions Act. It is a comprehensive act, so that the above-cited provisions are merely highlights. This Act is a very important contribution to computer information law, and should receive serious attention in every state.

APPENDIX B

July 9, 1999

Mr. John L. McClaugherty
Chair, Executive Committee
National Conference of Commissioners
on Uniform State Laws
211 E. Ontario Street, Suite 1300
Chicago, IL 60611

Dear Mr. McClaugherty:

As the National Conference of Commissioners on Uniform State Laws (NCCUSL) prepares to consider adoption of the Uniform Computer Information Transaction Act (UCITA), the staff of the Bureau of Consumer Protection and Competition and of the Policy Planning office of the Federal Trade Commission (FTC) wishes to express the same consumer welfare concerns that it raised in its October 30, 1998 letter to Carlyle C. Ring and Professor Geoffrey Hazard, Jr. about UCITA's predecessor, Uniform Commercial Code Article 2B (August 1, 1998 draft).¹ Those concerns, with one exception, have not been addressed in any significant respect in UCITA.² We briefly summarize the October 30, 1998 letter and have attached a copy for your convenience.

Although UCITA Section 105(b) now includes a public policy preemption provision, the language of the provision creates additional barriers to enforcing this public policy preemption that were not proposed in August 1, 1998 draft of Article 2B. Indeed, the new language of 105(b) only enhances the staff concerns enumerated in the October 30, 1998 letter.

UCITA endorses a license model for "computer information transactions."³ For example, under UCITA, a license to use software (rather than the sale of the software itself) would allow the licensor to limit or control how the license uses the software, even where the software has been mass-marketed to consumers. Examples of these limits or controls include

1. This letter represents the views of the Bureau of Consumer Protection and Competition and of the Policy Planning office and does not necessarily represent the views of the FTC or any individual Commissioner. the FTC, however, has authorized the staff to submit this letter.

2. The one exception is UCITA Section 816, which had no counterpart in Article 2B, that does address the staff's notice concerns about the use of electronic self-help by a licensor.

3. The Prefatory Note to UCITA defines "computer information transactions" to include transactions involving computer software, multimedia interactive products, computer data and databases, and Internet and online information.

restrictions on a consumer's right to sue for a product defect, to use the product, or even to publicly discuss or criticize the product.⁴

Unlike the law governing sales of goods, UCITA departs from an important principle of consumer protection that material terms must be disclosed prior to the consummation of the transaction. UCITA does not require that licensees be informed of licensing restrictions in a clear and conspicuous manner prior to the consummation of the transaction.⁵

For example, UCITA allows licensors of software to disclose these restrictions after the transaction has been completed, such as when the licensee opens the software box and discovers the terms of the license. Thus, in effect there may be no "meeting of the minds" prior to the consummation of the transaction. Moreover, UCITA adopts a definition of the term "conspicuous" that has the effect of allowing material license terms not to be disclosed clearly and conspicuously at any point before or after the transaction is completed.⁶

4. Although the actual provisions of UCITA itself do not expressly preempt or supplant any existing federal or state consumer protection laws and policies, the effect of these provisions is to allow licensors to enforce contract use restrictions in a mass market license that supplant many traditional terms of a contract that ordinarily are set by state and federal law.

5. Under Section 5 of the FTC Act, a misleading omission occurs "when qualifying information necessary to prevent a practice, claim, representation, or reasonable expectation or belief from being misleading is not disclosed." Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Associates, Inc.* 103 F.T.C. 110, 174 (note 4). This qualifying information must be made prior to purchase. The test of whether a misleading omission violates Section 5 of the FTC Act is whether "the omitted information would be a material factor in the consumer's decision to purchase the product." *Id.*, note 44.

6. UCITA's approach to "conspicuous" disclosure fails to take into consideration the context in which the disclosure is given. For example, UCITA includes several broad safe harbors in its definition of "conspicuous," so that, for example, a disclosure which is "in capitals in a size equal to or greater than, or in contrasting type, font, or color to, the surrounding text" (UCITA § 102(a)(15)(A)), would be considered conspicuous regardless of the context of the disclosure. Thus, under UCITA, a disclosure would be considered "conspicuous" even if such a disclosure were buried amid boiler-plate license text, or were printed on one of many different leaflets enclosed within a software box. This is the opposite approach the FTC has used to fulfill its law enforcement responsibilities. The term "clear and conspicuous" in FTC law refers to a general standard of effective communication. This standard is central to much of the case law that has developed under Section 5 of the FTC Act, 15 U.S.C. § 45, which empowers the FTC to take enforcement action against deceptive commercial practices. In order to determine whether this standard has been met, "the Commission considers the disclosure in the context of all the elements of the advertisement." FTC Request for Comment, Interpretation of Rules and Guides for Electronic Media, 63 Fed. Reg. 24996, 25002 (1998) (footnote omitted).

In addition, in its effort to establish a legal framework to facilitate electronic commerce, UCITA allocates significant risks to consumers in the event of unauthorized transactions. This, in turn, might deter, rather than advance, development of electronic commerce.

Further, UTICA expands the scope and power of contracts, particularly contracts designed by software vendors and intellectual property owners. The effect of such a change is potentially to provide state contract law with primacy over federal intellectual property laws in those cases where the licensor seeks to acquire or restrict rights beyond what federal or state law permits. For example, if a state were to adopt UCITA, state law could permit licensors to include anticompetitive grantback terms in a license that reduce the licensee's incentive to engage in research and development, unless the licensee took on the uncertain task of challenging the term subject to UCITA Section 105.⁷ By doing so, this could upset the delicate balance between intellectual property and competition policy, which has been carefully calibrated to recognize certain limits on intellectual property so as not to stifle competition or innovation. By allowing licensors of computer information to expand their rights, there is a possibility that these state-enforced contracts could restrain trade in violation of the antitrust laws, constitute misuse of intellectual property, and/or violate state trade secret statutes. As a result, UCITA may not have a neutral effect on competition policy.

In sum, we question whether it is appropriate to depart from these consumer protection and competition policy principles in a state commercial law statute, especially since many of these same principles are now being included as core elements in international e-commerce discussions. UCITA proposes these changes based on the implicit assumption that there is something unique about the technology involved (software and information access) that necessitates this departure from the traditional law of sales. If this is the case, we believe it would be more appropriate to seek a change to the underlying laws that are deemed to be inappropriate to software and other UCITA products. If a license model is deemed most appropriate nonetheless, the FTC staff in its October 30, 1998 letter recommended a number of changes to an earlier draft of UCITA which would help alleviate the staff's concerns.

7. See fn 2, *supra*.

It is our hope that the NCCUSL membership will consider the issues raised in the attached letter during deliberations over whether to adopt UCITA.

Respectfully submitted,

Joan Z. Bernstein, Director
Adam G. Cohn, Attorney
Division of Marketing Practices
Bureau of Consumer Protection
William J. Baier, Director
David A. Balto, Asst. Director for Policy and Evaluation
Bureau of Competition
Susan S. DeSanti, Director
Michael S. Wroblewski, Advocacy Coordinator
Policy Planning
FEDERAL TRADE COMMISSION
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580
cc: NCCUSL Members
Attachment

APPENDIX C

Article 5: Exceptions to the Restricted Acts

1. In the absence of specific contractual provisions, the acts referred to in Article 4(a) and (b) shall not require authorization by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction.

2. The making of a back-up copy by a person having a right to use the computer program may not be prevented by contract insofar as it is necessary for that use.

3. The person having a right to use a copy of a computer program shall be entitled, without the authorization of the rightholder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do.

Article 6: Decompilation

1. The authorization of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of Article 4(a) and (b) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

- (a) these acts are performed by the licensee or by another person having a right to use a copy of the program, or on their behalf by a person authorized to do so;
- (b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in subparagraph (a); and
- (c) these acts are confined to the parts of the original program which are necessary to achieve interoperability.

2. The provisions of paragraph 1 shall not permit the information obtained through its application:

- (a) to be used for goals other than to achieve the interoperability of the independently created computer programs;
- (b) to be given to others, except when necessary for the interoperability of the independently created computer programs; or
- (c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.

3. In accordance with the provisions of the Berne Convention for the Protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the rightholder's legitimate interests or conflicts with a normal exploitation of the computer program.

Article 9: Continued Application of Other Legal Provisions

1. The provisions of this directive shall be without prejudice to any other legal provisions such as those concerning patent rights, trademarks, unfair competition, trade secrets, protection of semiconductor products or the law of contract. Any contractual provisions contrary to Article 6 or to the exceptions provided for in Article 5(2) and (3) shall be null and void.

2. The provisions of this directive shall apply also to programs created before 1 January 1993 without prejudice to any acts concluded and rights acquired before that date.

-
1. American Bar Association Working Group Report on the Uniform Computer Information Transaction Act (“UCITA”), January 31, 2002, (hereinafter “January Report”).
 2. P. 7 of the January Report.
 3. Proposed 2002 Amendments to Uniform Computer Information Transactions Act, 2002 National Conference of Commissioners on Uniform State Laws.
 4. Council Directive of 14 May 1991 on the Legal Protection of Computer Programs, 91/250/EEC, O.J. (L/122) May 17, 1991 (*i.e.*, hereinafter “The Software Directive”).
 5. “Summary of the Uniform Computer Information Transactions Act” (*i.e.*, hereinafter “Summary”), 2000, National Council of Commissioners on Uniform State Laws; www.nccusl.org/uniformact_summaries/uniformacts-s-ucita.htm.
 6. Copyright preemption is provided under 17 U.S.C. § 301.
 7. In a case decided August 20, 2002, the U.S. Court of Appeals for the Federal Circuit held that a prohibition against reverse engineering contained in the shrinkwrap license for a computer aided design product was not preempted by the Copyright Act. Affirming a breach of contract verdict, the Court applied First Circuit law to find that the contract claim required an “extra element” of proof beyond that required to prove copyright infringement based on that court’s decision that a trade secret claim was not preempted. *Bowers v. Baystate Technologies Inc.*, 64 BNA’s PTCJ 401; *see also Wrench LLC v. Taco Bell Corp.*, 256 F.3d 446, 457 (6th Cir. 2001) (holding a state law contract claim not preempted by federal copyright law).
 8. See, *Step-Saver Data Sys. v. Wyse Technology*, 939 F.2d 91, 98-100 (3d Cir. 1991); *Arizona Retail Sys. v. Software Link, Inc.*, 831 F.Supp. 759, 764-766 (D. Ariz. 1993); *Specht v. Netscape Communications Corp.*, 150 F.Supp.2d 585 (S.D.N.Y. 2001); *Cf. ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) (concluding that a mass market transaction involving software was a “sale of goods” to which UCC Article 2 applied but nonetheless enforcing a “license agreement” under Article 2); and *i.LAN Systems, Inc. v. NetScout Service Level Corp.*, 183 F.Supp.2d 328 (D. Mass. 2002).
 9. “The Digital Millennium Copyright Act (DMCA) – Congress Responds to the Perceived Imbalance Between Content Providers and Users of Copyrighted Works Caused By Advances in Digital Distribution Technologies Including the Internet.”
 10. J. Thomas McCarthy, MCCARTHY’S DESK ENCYCLOPEDIA OF INTELLECTUAL PROPERTY, 2nd Edition 1991, 1995; *see also* THE FREE ON-LINE DICTIONARY OF COMPUTING (2001), at <http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?reverse+engineering>.
 11. *Kewanee Oil Co. v. Bicron Corp.*, 470 U.S. 470, 476 (1974).

-
12. “An author cannot acquire patent-like protection by putting an idea, process, or method of operation in an unintelligible format and asserting copyright infringement against those who try to understand that idea, process, or method of operation.” *Atari Games Corp. v. Nintendo of America, Inc.*, 975 F.2d 832, 842 (Fed. Cir. 1992).

“When the nature of a work requires intermediate copying to understand the ideas and processes in a copyrighted work, that nature supports a fair use for intermediate copying. Thus, reverse engineering object code to discern the unprotectable ideas in a computer program is a fair use.” *Id.* at 843.

“Allowing a computer programmer to hide his ideas, processes and concepts in a copyrighted object code defeats the fundamental purpose of the Copyright Act to encourage the creation of original works by protecting the creator’s expression while leaving the ideas, facts, and functional concepts in the free marketplace to be built upon by others.” *DSC Comm. Corp. v. DGI Technologies, Inc.*, 898 F.Supp. 1183, 1191 (N.D. Tex. 1995), *aff’d*, 81 F.3d 597 (5th Cir. 1996).
 13. *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 109 S.Ct. 971, 103 L.Ed.2d 118 (1989); *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 94 S.Ct. 1879, 40 L.Ed.2d 315 (1974).
 14. Restatement (Third) of Unfair Competition § 43 (1995) (hereinafter “Restatement”).
 15. Restatement (Third) of Unfair Competition § 43 comment b (1995).
 16. “[I]t is perfectly lawful for a competitor to buy a product embodying a trade secret and unmask the secret by reverse engineering fo the product. Only if the competitor (or anyone else for that matter) discovers the secret by breaking a contract or engaging in other unlawful or improper conduct can the individual or firm whose secret is was obtain a remedy.” *Micro Data Base Sys., Inc. v. Dharma Sys., Inc.*, 148 F.3d 649, 657 (7th Cir. 1998).
 17. *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1527 (9th Cir. 1992).
 18. *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000).
 19. *Supra*, Note 4.
 20. *Supra*, Note 3.