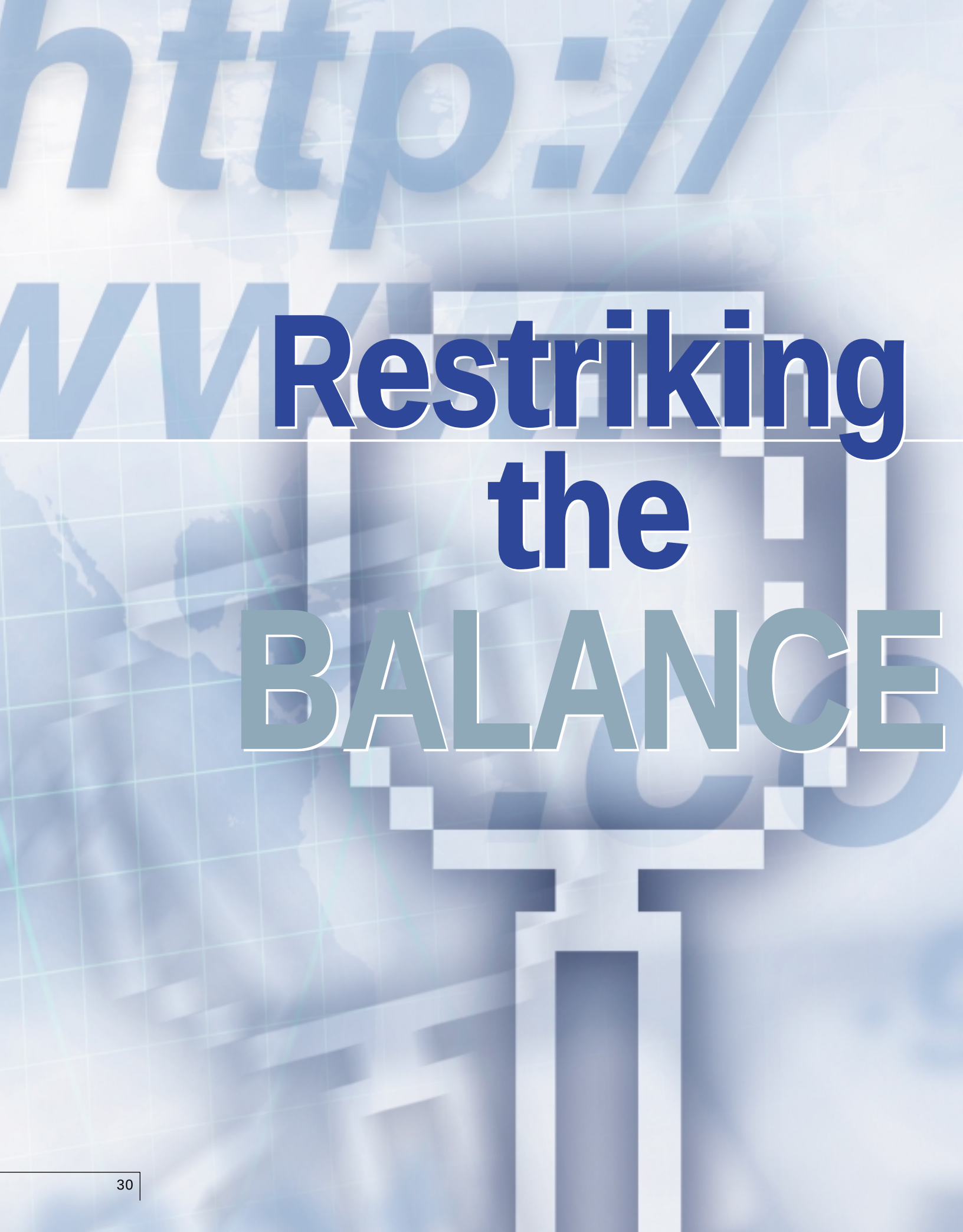
http://
Restriking
the
BALANCE

The Uniform Computer Information Transactions Act (UCITA) and Reverse Engineering

By David Syrowik

Editorial Note: As this article was going to press, a related event occurred. On February 10, 2003, the NCCUSL withdrew a resolution approving UCITA, which was before the ABA House of Delegates. NCCUSL's president cited "requests by a number of ABA sections and leaders to defer an extensive debate" on the merits of the act when "it became evident that a clear consensus on the act was unlikely to emerge." ABA approval is a "customary step in the process of passing proposed uniform laws such as UCITA." See http://www.nccusl.org/nccusl/ucita/UCITA_ABA_0203.pdf and http://www.itworld.com/Man/2681/030212ucita/pfindex.

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 law....*[2]

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 amendments[3] 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 article reviews the law of reverse engineering and then compares new section 118 with the reverse engineering provisions of the European Community (EC) Directive on the Legal Protection of Computer Programs[4] to which new section 118 has been compared by the standby committee.

UCITA and its Relation to Intellectual Property Law

In 2000, the NCCUSL summarized UCITA.[5] In the 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 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 USC 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.*

In a letter dated July 9, 1999, the Federal Trade Commission (FTC) attacked UCITA.[6] 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

Fast Facts:

UCITA gives courts the power and responsibility to reconcile commercial licensing law with intellectual property law, most of which is federal in origin.

Reverse engineering is defined as, "the process of starting with the known product and working backwards to divine the process that aided in its development or manufacture."

The U.S. 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 the product on the open market.

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 . . . ."

Reverse Engineering

The term "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 that aided in its development or manufacture."[7]

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

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.[8]

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).

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"...

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 the product on the open market.[9]

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."[10]

> *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 discover 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.*[11]

A "duty of confidence" can arise through contract such as a license agreement having a confidentiality provision,[12] 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.

The leading case involving the reverse engineering of computer programs in the U.S. is the *Sega* case.[13] 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."

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.[14] 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.

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.

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."

On May 14, 1991, the European Community (EC) adapted its Software Directive.[15] Articles five, six, and nine of the Software Directive are relevant to the issue of reverse engineering of computer programs. In general, the Software Directive strictly limits not only when reverse engineering will be tolerated, but also how the information obtained by reverse engineering can be utilized.

Article five sets forth the terms and conditions required for reverse engineering other than decompilation.

Article six of the Software Directive permits decompilation to achieve interoperability "with other programs." Consequently, a compatible program created using information derived through decompilation may compete with the decompiled program insofar as it interoperates with other programs in the same way that the decompiled program does. One may not decompile a computer program solely to research its underlying ideas unrelated to interoperability. Under article nine, the exceptions provided in article five and article six cannot be overridden by contract.

New section 118 is as follows:

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).[16]

The above language provides a right to reverse engineer very analogous to the right provided by the Software Directive.

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."

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 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. ✦

David Syrowik is a patent attorney with the Southfield firm of Brooks & Kushman P. C. He serves on the council of the Computer Law Section of the State Bar. He is chair of that section's Proprietary Rights Committee and Writing Award Contest. Dave also is an adjunct professor of law at UD Mercy Law School where he teaches a course in Computer and Internet Law.

Footnotes

1. American Bar Association Working Group Report on the Uniform Computer Information Transaction Act ("UCITA"), January 31, 2002, (hereinafter "January Report"). http://www.abanet.org/leadership/ucita.pdf.
2. P. 7 of the January Report. http://www.law.upenn.edu/bll/ulc/ucita/UCITA_amds_AM02.htm.
3. Proposed 2002 Amendments to Uniform Computer Information Transactions Act, 2002 National Conference of Commissioners on Uniform State Laws. http://pf-lj.kelt.si/internetinpravo/pr_viri/DirektivaESRP.htm.
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") (c) 2000, National Council of Commissioners on Uniform State Laws; www.nccusl.org/uniformact_summaries/uniformacts-s-ucita.htm.
6. "Letter From the Federal Trade Commission Bureau of Consumer Protection, Bureau of Competition, and Policy Planning Office." www.ftc.gov/be/v990010.htm.
7. *Kewanee Oil Co v Bicron Corp*, 470 US 470, 476 (1974).
8. *Atari Games Corp v Nintendo of America, Inc*, 975 F2d 832, 842 (Fed Cir 1992); *DSC Comm Corp v DGI Technologies, Inc*, 898 F Supp 1183, 1191 (ND Tex 1995), aff'd, 81 F3d 597 (CA 5, 1996).
9. *Bonito Boats, Inc v Thunder Craft Boats, Inc*, 489 US 141, 109 S Ct 971, 103 L Ed 2d 118 (1989); *Kewanee Oil Co v Bicron Corp*, 416 US 470, 94 S Ct 1879, 40 L Ed 2d 315 (1974).
10. Restatement (Third) of Unfair Competition § 43 (1995) (hereinafter "Restatement").
11. Restatement (Third) of Unfair Competition § 43 comment b (1995).
12. *Micro Data Base Sys, Inc v Dharma Sys, Inc*, 148 F3d 649, 657 (CA 7, 1998).
13. *Sega Enters Ltd v Accolade, Inc*, 977 F2d 1510, 1527 (CA 9, 1992).
14. *Sony Computer Entertainment, Inc v Connectix Corp*, 203 F3d 596 (CA 9, 2000).
15. Supra, note 4.
16. Supra, note 3.