CLOSING THE INTEROPERABILITY GAP: NCCUSL'S ADOPTION OF A REVERSE ENGINEERING EXCEPTION IN UCITA

by

Jonathan Band[1]

On December 17, 2001, the Standby Committee for the Uniform Computer Information Transactions Act (UCITA) issued a report which recommended adoption of a reverse engineering exception in UCITA.[2] The Executive Committee of the National Conference of Commissioners on Uniform State Laws (NCCUSL) subsequently ratified this recommendation. With this decision, the United States has finally caught up to the European Union's favorable legal treatment of software interoperability.

I. Contractual Restrictions on Reverse Engineering

More than a decade ago, the European Union promulgated its Software Directive,[3] which provided software developers in Europe a high degree of certainty concerning the scope of copyright protection for programs. In particular, the Software Directive clearly limited copyright protection when it would prevent interoperability. Article 6 permitted the reverse engineering technique known as decompilation[4] for purposes of achieving interoperability; Article 7 contained a reverse engineering exception to the prohibition on

[1] Jonathan Band is a partner in the Washington, D.C. office of Morrison & Foerster LLP. He has represented interoperable software developers with respect to some of the matters discussed in this article.

[2] Prior to the adoption of UCITA by the NCCUSL, the UCITA Standby Committee was the UCITA Drafting Committee.

[3] Council of Ministers Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs, 1991 O.J. (L 122) 42.

[4] Decompilation or disassembly involve translating machine readable object code into a higher level, human readable form. *See* Band & Katoh, *Interfaces on Trial: Intellectual Property and Inteoperability in the Global Software Market* (Westview Press 1995) at 12-17.

the circumvention of technological protection measures; and Article 9(1) provided that a contractual restriction on the reverse engineering exception was "null and void."

Since the promulgation of the Directive in 1991, the United States has been playing catch-up to the European Union. In 1992, the U.S. Court of Appeals for the Ninth Circuit found 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." *Sega Enters v. Accolade Inc.*, 977 F.2d 1510, 1527-28 (9th. Cir. 1992). In *Sega*, the court concluded that achieving interoperability between the Accolade games and the Sega game console was such a legitimate reason.[5]

In 1998, seven years after the Software Directive, the U.S. tackled the circumvention issue in the Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (DMCA). 17 U.S.C. Section 1201(f) contains a reverse engineering exception to the circumvention prohibitions of Sections 1201(a) and (b). Interestingly, much of the language for Section 1201(f) comes from Article 6 of the Software Directive.

That left contractual restrictions on reverse engineering. This was a real problem because most software is distributed subject to a license of some sort, and many of these licenses prohibit reverse engineering for any reason. Prior to the December 17, 2001 Standby Committee Report, the enforceability of such provisions, particularly in shrinkwrap licenses,[6] was uncertain. Although strong arguments could be raised against their enforceability, no one approach gained wide acceptance in the courts.

---

[5] *See also Atari Games Corp. v. Nintendo of America, Inc.*, 975 F.2d 832 (Fed. Cir. 1992); *Bateman v. Mnemonics*, 79 F.3d 1532 (11th Cir. 1996); and *Sony Computer Entertainment, Inc. v. Connectix Corp*., 203 F.3d 596 (9th Cir. 2000).

[6] A shrinkwrap license is printed on or within the plastic wrapping enclosing a software product. According to most shrinkwrap licenses, the licensee agrees to its terms by tearing the plastic shrinkwrap, which the licensee must do to use the product

II. Preemption

In 1988, three years *before* the promulgation of the Software Directive, the U.S. Court of Appeals for the Fifth Circuit set aside a contractual restriction on reverse engineering in *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255 (5th Cir. 1988). The *Vault* court cited *Sears, Roebuck & Co. v. Stiffel Co*., 376 U.S. 225 (1964), where the Supreme Court relied on the U.S. Constitution's Supremacy Clause to conclude that "[w] hen state law touches upon an area of [the copyright statutes], it is 'familiar' doctrine' that the federal policy 'may not be set at naught, or its benefits denied' by state law." *Sears*, 376 U.S. at 229 (citations omitted). The *Vault* court held that a reverse engineering prohibition in a shrinkwrap license "conflicts with the rights of computer program owners under Section 117 and clearly 'touches upon an area' of federal copyright law." *Vault*, 847 F.2d at 270.

In the thirteen years since *Vault*, courts have used the Supremacy Clause to preempt state statutes inconsistent with the federal intellectual property system, *e.g*., the Florida plug mold statute in *Bonito Boats Inc., v. Thunder Craft Boats Inc.*, 489 U.S. 141 (1989). However, no court has specifically adopted the *Sears/Vault* reliance on the Supremacy Clause to find unenforceable a contractual provision that conflicts with a user privilege recognized by the Copyright Act, such as Section 107's fair use doctrine.

At the same time, some courts have ruled that the preemption provision of the Copyright Act, 17 U.S.C. Section 301(a), *does not* preempt contract terms. Section 301(a) preempts state laws creating "rights that are equivalent to any of the exclusive rights within the general scope of copyright...." Courts have interpreted Section 301(a) as not preempting a state cause of action which requires proof of "extra elements" not present in a copyright claim. The Seventh Circuit in *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996)

ruled that Section 301(a) did not preempt enforcement of a contract prohibiting the copying of telephone listings because the contract claim required proof of an extra element -- the existence of an enforceable contract.

On the other hand, some scholars have rejected the *ProCD* analysis:

> [A]t times a breach of contract cause of action can serve as a subterfuge to control nothing other than the reproduction, adaptation, public distribution, etc. of works within the subject matter of copyright. That situation typically unfolds when the "contract" at issue consists of a "shrinkwrap license" to which the copyright owner demands adhesion as a condition to licensing its materials. To the extent that such a contract is determined to be binding under state law, then that law may be attempting to vindicate rights indistinguishable from those accorded by the Copyright Act. Under that scenario, the subject contract cause of action should be deemed pre-empted .... Although the vast majority of contract claims will presumably survive scrutiny ... nonetheless pre-emption should strike down claims that, although denominated "contract," nonetheless complain directly about the reproduction of expressive materials.

1 Melville B. Nimmer & David Nimmer, NIMMER ON COPYRIGHT, § 1.01[B][1][a] at 1-19 and 1-22 (2001) (citations omitted).

Relying on this passage, the court in *Selby v. New Line Cinema*, 96 F. Supp. 2d 1053 (C.D. Cal. 2000), declined to enforce an implied-in-fact contract prohibiting the use of an idea without attribution. Similarly, the court in *Symantec Corp. v. McAffee Assocs., Inc.*, No. C-97-20367, 1998 WL 740798 (N.D. Cal. June 9, 1998), declined to enforce a contractual restriction on reverse engineering. The court found that the mere existence of the agreement was insufficient to transform "what essentially is a copyright infringement claim" into "something more."

In short, the contours of both Constitutional and Section 301(a) preemption of contractual restrictions on otherwise lawful reverse engineering have not yet been determined definitively.

III. Misuse

The copyright misuse doctrine is premised on the notion that public policy "forbids the use of the [copyright] to secure an exclusive right or limited monopoly not granted by the [Copyright] Office and which it is contrary to public policy to grant." *Lasercomb America, Inc. v. Reynolds*, 911 F.2d 970, 977 (4th Cir. 1990)(citations omitted). One court has relied on the copyright misuse doctrine to refuse enforcement of a contractual restriction on reverse engineering.

In *Alcatel U.S.A., Inc., v. DGI Techs., Inc*. 166 F.3d 772 (5th Cir. 1999), DSC developed both an operating system and a microprocessor card for a telecommunications switch. Running the operating system required copying it into the microprocessor's memory. DGI developed microprocessor cards compatible with the DSC operating system. To test and to use the DGI cards, the DSC operating system had to be loaded into the cards' memory. The DSC license agreement, however, prohibited the running of the DSC operating system on non-DSC cards. The jury found that DSC's license agreement constituted copyright misuse, and the Fifth Circuit agreed with its finding: "DSC has used its copyright to indirectly gain commercial control over products DSC does not have copyright, namely its microprocessor cards." *Alcatel*, 166 F.3d at 793.

In an earlier decision in the same case, the Fifth Circuit ruled that DSC's license likely constituted copyright misuse because "DSC seems to be attempting to use its copyright to obtain a patent-like monopoly over unpatented microprocessor cards." *DSC Communications Corp. v. DGI Techs. Inc.*, 81 F.3d 597, 601 (5th Cir. 1996). The Court reasoned:

> Any competing microprocessor card developed for use on DSC phone switches must be compatible with DSC's operating system software. In order to ensure that its card is compatible, a competitor such as DGI must test the card on a DSC phone switch. Such a test necessarily involves making a copy of DSC's copyrighted operating system, which copy is downloaded into the card's memory

> when the card is booted up. If DSC is allowed to prevent such copying, then it can prevent anyone from developing a competing microprocessor card, even though it has not patented the card.

Id.

Although the copyright misuse doctrine is gaining acceptance, it is still relatively new, and *Alcatel* is one of the few cases where copyright misuse has been found. Thus, it does not yet provide software developers with the certainty they need to commit significant resources to the reverse engineering necessary for the development of new interoperable products.

IV. Contract Arguments

In addition to preemption and misuse, arguments concerning the validity of the contract can be made with respect to shrinkwrap or click-on[7] licenses. Because a user cannot use a program without "agreeing" to these license terms either by opening the package or clicking the "I agree" icon, significant questions arise whether the user has in fact manifested assent to the license's terms.

Courts around the country have just begun to consider the enforceability of shrinkwrap and click-on licenses, and a consensus has not yet emerged.[8] Moreover,

---

[7] A click-on license appears when a user is installing a program on his computer. The user must click on an "I agree" icon in order to complete the installation sequence.

[8] *Compare Novell, Inc. v. Network Trade Ctr., Inc*., 25 F. Supp. 2d 1218, 1230 (D. Utah 1997); *Morgan Labs., Inc. v. Micro Data Base Sys., Inc*. 41 U.S.P.Q.2d 1850 (N.D. Cal. 1997); *Arizona Retail Sys., Inc. v. The Software Link, Inc*., 831 F. Supp. 759, 764-66 (D. Ariz. 1993); *Step-Saver Data Sys. v. Wyse Tech*., 939 F.2d 91, 98-100 (3d Cir. 1991); *Foresight Resources Corp. v. Pfortmiller,* 719 F. Supp. 1006, 1010 (D. Kan. 1989); *Ticketmaster Corp. v. Tickets.com, Inc*., 2000 U.S. Dist. LEXIS 12987 (C.D. Cal. August 10, 2000), *aff'd*, 248 F. 3d 1173 (9th Cir. 2001); *Specht v. Netscape Communications Corp*., 150 F. Supp. 2d 585, 596 (S.D.N.Y. 2000); *Softman Prods. Co. v. Adobe Systems, Inc*., 171 F. Supp. 2d 1075 (C.D. Cal. 2001); and *Klocek v. Gateway, Inc*., 104 F. Supp. 2d 1332, 1338-39 (D. Kan. 2000); *with ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996); *cf. Hill v. Gateway 2000, Inc*., 105 F.3d 1147, 1150 (7th Cir. 1997), *cert. denied*, 522

numerous commentators have questioned the enforceability of such contracts.[9] If the contracts are not enforceable, then obviously their terms prohibiting reverse engineering have no effect.

This is where UCITA enters the picture. A fundamental goal of UCITA is to render shrinkwrap and click-on licenses clearly enforceable as a matter of state contract law. Thus far, UCITA has been adopted only in two states, Maryland and Virginia, and has encountered opposition from state attorneys general, organized groups of licensees, the American Law Institute, the Federal Trade Commission, and the American Bar Association. Nonetheless, NCCUSL remains committed to the adoption of UCITA in all 50 states. Additionally, even in states where UCITA has not been adopted, courts might look to UCITA and its lengthy comments as an authoritative statement concerning contract law in the digital age.

Accordingly, UCITA has weakened the strength of the argument that shrinkwrap and click-on licenses are unenforceable as a matter of state contract law. For this reason,

---

U.S. 808 (1997).

[9] *E.g.*, Michael J. Madison, *"Legal Ware": Contract and Copyright in the Digital Age*, 67 FORDHAM L. REV.1025 (Dec. 1998); Robert J. Morrill, Comment, *Contract Formation and the Shrink Wrap License: A Case Comment on ProCD, Inc. v. Zeidenberg*, 32 NEW ENG. L. REV. 513, 537-50 (1998); Apik Minassian, *The Death of Copyright: Enforceability of Shrinkwrap Licensing Agreements*, 45 UCLA L. REV. 569 (1997); Jason Kuchmay, Note, *ProCD, Inc. v. Zeidenberg: Section 301 Copyright Preemption of Shrinkwrap Licenses - A Real Bargain for Consumers?*, 29 U. TOL. L. REV. 117 (1997); Kell Corrigan Mercer, Note, *Consumer Shrink-Wrap Licenses and Public Domain Materials: Copyright Preemption and Uniform Commercial Code Validity in ProCD v. Zeidenberg*, 30 CREIGHTON L. REV. 1287 (1997); Christopher L. Pitet, Comment, *The Problem With "Money Now, Terms Later": ProCD, Inc. v. Zeidenberg and the Enforceability of "Shrinkwrap" Software Licenses*, 31 LOY. L.A. L. REV. 325 (1997); Stephen P. Tarolli, Comment, *The Future of Information Commerce Under Contemporary Contract and Copyright Principles*, 46 AM. U. L. REV. 1639 (1997); Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239 (1995), supra note 10, at 1248-59; L. Ray Patterson & Stanley W. Lindberg, *The Nature of Copyright: A Law of Users' Rights*, 220 (1991).

entities interested in preserving the reverse engineering privilege attempted to persuade the UCITA drafters to adopt an explicit reverse engineering exception.

V. UCITA and Reverse Engineering

Initially, the UCITA drafters took the position that any conflict between UCITA and the federal Copyright Act was addressed by the general preemption provision included in UCITA: "A provision of this Act which is preempted by federal law is unenforceable to the extent of the preemption." Section 105(a). In an effort to rebut criticism of UCITA, some UCITA proponents asserted that under this provision, a contractual term that attempted to limit a privilege granted under the Copyright Act was *per se* unenforceable. The UCITA reporter's comments, however, noted that "[e]xcept for rules that directly regulate specific contract terms, no general preemption of contracting arises under copyright or patent law." Comment 105(2). In other words, the Copyright Act as a general matter does *not* preempt contract terms. The comment observes that preemption only occurs when the Act specifically prohibits a particular term, or in other situations recognized by the evolving case law.

Advocates of user privileges, including reverse engineering, argued that the limited and uncertain scope of preemption, acknowledged in the reporter's comment, rendered preemption a questionable means of preserving user privileges in an era where the distribution of content subject to shrinkwrap or click-on license was increasingly prevalent. A decade or more could pass until the Supreme Court rules on whether a shrinkwrap license term limiting a user privilege under the copyright laws impermissibly interferes with the federal intellectual property system. In the meantime, courts in UCITA jurisdictions would enforce the license terms.

In response to this argument, NCCUSL adopted Section 105(b), which permits public policy invalidation:

> If a term of a contract violated 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 reporter's comments to this provision explicitly discuss reverse engineering.

> This Act does not address ... 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. Section 1201 (1999). It expressly addresses reverse engineering and security testing in connection with circumvention of technological protection measures that limit access to copyrighted works. It recognizes a policy not to prohibit some reverse engineering where it is needed to obtain interoperability of computer programs....It further recognizes a policy to not prohibit security testing where it is needed to protect the integrity and security of computers, computer systems or computer networks ....This policy may outweigh a contract term to the contrary.

Comment 105(3).

Without question, Section 105(b) combined with the reporter's comments provided some comfort to developers of interoperable software. This comfort, however, was limited. First, the comment is very cautious; it implies that reverse engineering for purposes of achieving interoperability is a fundamental public policy, but does not say so explicitly. Second, the reporter's comments have no legal status; a court is not required to give them any weight. Thus, notwithstanding the comments' implications, there is no guaranty that a court will in fact conclude that reverse engineering for purposes of interoperability is a fundamental public policy.

Third, even if a court does conclude that reverse engineering is a fundamental public policy, it still must balance that policy against the policy favoring enforcement of contracts. 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 a very high standard to meet. The comment suggests that reverse engineering "*may* outweigh a contract term to the contrary," but does it *clearly* outweigh a term to the contrary?

In the face of this uncertainty, supporters of reverse engineering continued to press for an express exemption, even after NCCUSL adopted UCITA in 1999, and after UCITA was enacted in Virginia and Maryland in 2000. In November, 2001, the UCITA Standby Committee held an open meeting in Washington, D.C., to consider possible amendments to the official text of UCITA. Several amendments relating to reverse engineering were proposed and debated at the meeting.

On December 17, 2001, the Standby Committee issued a report that recommended adopting the following new section concerning reverse engineering:

> Section 115. Terms on Reverse Engineering
>
> (a) Notwithstanding the terms of a contract under 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 which are necessary to achieve interoperability of an independently created computer program with other programs, 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 other law.
>
> (b) 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.

Standby Committee Report Recommendation 19 at 25. The report's comment on Section 115 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." *Id.* at 25-26. And indeed, the language of Section 115 is very similar to that of the reverse engineering exception in Section 1201(f) of the DMCA, which in turn is similar to the language of Article 6 of the EU Software Directive. Thus, Section 115 harmonizes U.S. law with that of the EU.

In January, 2002, the NCCUSL Executive Committee adopted this recommendation, along with the other amendments proposed in the December report. The amendments will be considered by all the NCCUSL commissioners at the annual meeting during the summer of 2002.

VI. Conclusion

Although strong arguments could be made that the Constitution or the Copyright Act preempt enforcement of contractual restrictions on reverse engineering, or that such terms are a form of copyright misuse, the law on these points is far from settled. Moreover, UCITA undermines arguments that shrinkwrap licenses are not enforceable because the licensees do not really assent to their terms. For this reason, the new Section 115 of UCITA is most welcome. It establishes a bright line rule for software developers to follow. As such, it will promote interoperability, and hence competition, in the software industry. It also levels the legal playing field between the U.S. and the EU.