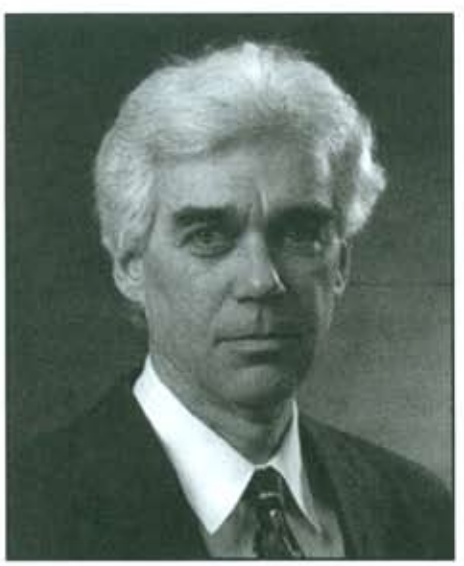
Volume 31, Number 1 » 2006

THE INTELLECTUAL PROPERTY LAW SECTION OF THE STATE BAR OF CALIFORNIA

NewMatter

Official Publication of The Intellectual Property Law Section of the State Bar of California

Circuit Court Decisions Weaken, Strengthen Hand of Software Owners Using Technological Protection Measures



Mitchell Zimmerman
Fenwick & West LLP

Within one late summer week, two federal Courts of Appeals rendered decisions that will have a significant effect on the rights of copyright holders. In both cases, third parties had overcome password schemes that software owners employed to protect their works from use by unauthorized parties. The Federal Circuit spurned the resulting claims in the first case; the Eighth Circuit embraced them in the second.

In *Storage Technology v. Custom Hardware Engineering*,[1] a divided panel of the Federal Circuit weakened the position of software copyright owners by reading expansively the right to copy that 17 U.S.C. § 117(c) gives independent service operators, and reading narrowly an express contractual term that sought to preclude other-party use of plaintiff's maintenance program. One week later, in *Davidson & Associates v. Jung*,[2] the Eighth Circuit strengthened the hand of software owners, interpreting the Digital Millennium Copyright Act's circumvention bar expansively and upholding a contractual prohibition on reverse engineering against a preemption challenge. In December 2005, StorageTek's petition for rehearing *en banc* was denied, but the original panel concurrently issued a further opinion that confirmed the original outcome.[3]

see *Circuit Court* page 5

inside

Circuit Court

CONTINUED FROM PAGE 1

STORAGETEK V. CUSTOM HARDWARE ENGINEERING

The plaintiff in the Federal Circuit's *StorageTek* case sold large data storage systems comprised of automated tape cartridge libraries and computers and software that ran the libraries and the overall system. "Maintenance Code" software was pre-loaded on the systems, but was not licensed to the purchasers—indeed, the license for plaintiff's other software for the storage system expressly provided that the purchaser acquired no rights to use the maintenance code. The Maintenance Code booted up automatically when the system was turned on, but the program and its diagnostic data were protected by a password scheme that kept anyone but StorageTek maintenance employees from accessing and using Maintenance Code.

Defendant Custom Hardware Engineering ("CHE") was an independent service organization in competition with StorageTek for the business of servicing StorageTek systems. CHE circumvented the password protection measures, then used the diagnostic data generated by the Maintenance Code in order to provide maintenance for the StorageTek systems.

StorageTek sued CHE, alleging that CHE infringed StorageTek's Maintenance Code copyrights when it booted up the system for servicing (thereby making a copy of the software in RAM), that CHE violated the DMCA when it circumvented StorageTek's password protection, and that CHE breached StorageTek's trade secrets in the fault codes that carried diagnostic information about the system when it used them for servicing.

The Federal Circuit rejected the copyright infringement claim on two grounds: first, that CHE was entitled to create the RAM copy under the Computer Maintenance Competition Assurance Act (codified at 17 U.S.C. § 117(c)); and second, that CHE was impliedly licensed to make the copy under StorageTek's agreements with the purchasers of the systems.

The § 117(c) Defense to RAM Copying.

Section § 117(c) provides that it is not an infringement for one authorized by the owner of a machine to make a copy of a computer program, if it is made "solely by virtue of activation of a machine…for purposes only of maintenance or repair of that machine." The defense under § 117(c) is subject to two further conditions: (1) that the new copy, created as a result of activating the machine, "is used in no other manner and is destroyed immediately after the maintenance or repair is completed; and (2) with respect to any computer program or part thereof that is not necessary for the machine to be activated, such program or part thereof is not accessed or used other than to make such new copy by virtue of the activation of the machine." The Federal Circuit rejected StorageTek's arguments that CHE was not shielded from liability by § 117(c).

StorageTek contended that CHE's activities did not comport with either proviso of § 117(c). First, StorageTek argued that CHE was not eligible under § 117(c) because CHE did not—as required by § 117(c) condition (1)—destroy the copy of the Maintenance Code "immediately" after completion of repair or maintenance; indeed, the copy of Maintenance Code that CHE used was kept in RAM for the entire period of CHE's service contract. But "maintenance," the Federal Circuit held, is a continuous process that includes ongoing monitoring of system performance. Destruction of the RAM copy at the conclusion of the service contract was therefore "immediate" enough, and the copy did not need to be destroyed before then.

StorageTek also maintained that CHE's use of the diagnostic Machine Code was inconsistent with condition (2) of § 117(c). This provides that if a copy is made of "any computer program or part thereof that is not necessary" for the machine to be activated, it may "not [be] accessed or used other than to make such new copy by virtue of the [machine's] activation." StorageTek argued that since the Maintenance Code's functions were diagnostic and maintenance-oriented in nature, the Maintenance Code was not necessary for the machine to be activated. Since CHE did access and use the fault symptom codes generated by the maintenance software in order to perform system maintenance, it was disqualified from the benefit of § 117(c).

The *StorageTek* majority acknowledged that accessing freestanding diagnostic programs would violate the condition set forth in § 117(c)(2), making the defense unavailable. This conclusion was unavoidable in light of the legislative history, never referred to by the court, which specifically uses maintenance programs as examples of programs not necessary for machine activation. Notwithstanding, the court held, because the Maintenance Code and what it called the "functional code" that operated the storage system were thoroughly entangled, loading the Maintenance Code into RAM was "necessary" to activate the machine, and condition (2) did not consequently bar the § 117(c) defense.

The Federal Circuit's convoluted argument never actually explained why "entanglement" should make a program—or, as the statute provides, a "part thereof"—necessary for machine activation within the meaning of the statute. That the disputed application program is configured to actually launch when the system boots up, creating a RAM copy, can scarcely be sufficient to show that a program is "necessary" for machine activation. If that were the case, copies created "by virtue of activation" of a computer would always

be "necessary," and condition (2) could never come into play. Further, condition (2) of § 117(c) specifically anticipates situations in which *"part"* of a program may not be necessary for machine activation (and bars accessing or using that part if the defense is to apply). No matter how interwoven the different parts of the code might be, consequently, the statute obviously contemplates that in the end we consider whether there is a part of the program that boots up which is not *necessary* for machine activation, and whether the defendant is accessing or using that part. In this case, whether entangled with functional code or not, the part of the code performing maintenance functions was not necessary for machine activation, so—under condition (2)—CHE could not use that part of the program and still be shielded from the infringement claim. CHE did so, therefore § 117(c) should not have protected its copying.

The Federal Circuit also ignored the point that condition (1) of § 117(c) makes the defense unavailable unless the new copy created by machine activation is used in "no other manner" than machine activation. CHE did use the copy in another manner, *viz.*, to obtain information (diagnostic fault messages) it used to maintain the StorageTek systems. It was therefore not entitled to make a copy of Maintenance Code under the terms of § 117(c).

In its December 2005 opinion, the panel (divided as in the original decision) offered "a brief additional discussion" on the § 117(c) issue. Again, the panel asserted that "determining whether a particular piece of software is 'necessary for [the] machine to be activated' is not a simple task." Since, the court reasoned, the part of the code that was required to boot up the machine was intertwined with the maintenance code, even if the maintenance code could later be deactivated, this "does not change the fact that a copy of the entire maintenance code must be loaded into RAM when the machine is turned on."

The court's additional discussion remains as flawed as its original treatment of this issue. First, again, that a part of the code was in fact loaded when the machine was activated does not mean that that part was *necessary* for machine activation. Second, the court ignores § 117(c)'s requirement in condition (1) that "such new copy" (the copy "made solely by virtue of activation" of the computer) be "*used in no other manner*...." CHE's manner of use of the maintenance code went beyond its inevitable creation when the StorageTek system was activated; CHE used the code thereafter for maintaining the system. Regardless of whether the initial making of the copy was privileged under § 117(c), CHE's subsequent exploitation of that copy breached § 117(c)'s clear requirement that independent service providers not *use* a copied program except to activate the machine.

The Federal Circuit's Implied License Ruling.

In an equally strained alternative holding, the Federal Circuit also found that, notwithstanding contract language that specifically excludes use of the maintenance code, purchasers were entitled both to load the code and to authorize others to use it. Nonetheless, the majority concluded that because the code would be copied automatically when the machine was turned on, equipment owners were necessarily authorized to use the code.

Various provisions of the agreement, the court argued, implied that "the license is tied to the piece of equipment on which the software resides." The court pointed, for example, to a provision that owners of the equipment "'may transfer possession of Internal Code only with the transfer of the Equipment on which its use is authorized,'" and the court also noted that the "license grants the customer the use of the code for 'the sole purpose of enabling the specific unit of Equipment for which the Internal Code was provided.'" But the fact that the license and equipment are "tied," for some stated purposes, simply does not imply that anyone starting up the machine—even if impliedly authorized to load the Maintenance Code into RAM as part of the start-up process—was authorized to *use* that code in order to perform maintenance. Any such implication is also negated by the fact that there was no license to the Maintenance Code to be tied to the equipment. The StorageTek software license (not quoted in the decision) expressly provided that it "confers [on the purchaser of the storage system] *no license or other right to use Maintenance Code.*"[4] It is difficult to square the purported implied license granting a right to use with the express contractual negation of any such right.

Responding to the court's analysis that tied the Internal Code license to the equipment, StorageTek's rehearing petition pointed out that the license's definition of "Internal Code" excluded Maintenance Code. The court dealt with this through denial: "Our decision [the December 2005 opinion states] did not rest on an interpretation of the term 'Internal Code,' but rested instead on our conclusion that permission to copy StorageTek's software was implicit in the licensing agreement, which permits the licensee to activate the equipment." The argument is disingenuous because the panel plainly *had* relied on the provisions concerning Internal Code as the basis for its analysis that an implied license was tied to the equipment. Second, again, the asserted implied authorization to create a copy of Maintenance Code by activating the equipment is an entirely different matter from any implied contractual right to *use* or authorize another to *use* that code, especially in the face of an express provision to the contrary.

The key lesson of the *StorageTek* contract analysis would seem to be that software owners' license agreements must be extraordinarily explicit about the point if they want to bar third-party use. This is

a disturbing conclusion because—up to this decision—few readers would have found much ambiguity in a license including the language employed by StorageTek with regard to its Maintenance Code.

Looking at the big picture under § 117(c), the Federal Circuit seems to have missed the point. Section 117(c) was intended to prevent computer system manufacturers from leveraging their system software copyrights into monopolies on maintenance services, merely because their maintenance programs loaded automatically when the systems booted up. That is, independent service providers should not be considered infringers just because they unavoidably copied a program without authorization when that program automatically launched at system startup. But the fundamental issue in *StorageTek* was not whether CHE could merely turn on the StorageTek machines in order to service them. The issue was whether CHE was entitled to a free ride—to *use* StorageTek's maintenance program to provide maintenance services rather than developing and using its own program. Particularly in light of the legislative history indicating Congress's intent *not* to allow independent service operators to actually use copyright holders' maintenance programs, the policy reason for the outcome is hard to fathom.

The Circumvention and Trade Secret Claims.

The Federal Circuit disposed of the two remaining issues, StorageTek's circumvention claim and its trade secrets claim.

In its holding in a 2004 case, *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*,[5] the Federal Circuit had held that circumventing an access-controlling technological protection measure was only unlawful if the circumvention "infringes or facilitates infringing a right protected by the Copyright Act." Since the court had concluded in *StorageTek* that CHE's copying was protected by § 117(c), CHE could not be liable for circumvention. The ruling confirms an important point: Although a number of other courts have held to the contrary, under *Chamberlain* and *StorageTek,* defenses to the underlying copyright infringement are defenses to circumvention claims. If this is the case for the § 117(c) defense, there would be no apparent reason to treat fair use or any other defense differently.

Finally, regarding the trade secret claim, the court held there was no violation because (1) the fault symptom codes generated by StorageTek's Maintenance Code had themselves not previously been kept secret, and (2) the reasons a particular machine no longer owned by StorageTek is malfunctioning cannot be a secret.

DAVIDSON & ASSOCIATES V. JUNG

In the Eight Circuit's *Davidson* decision, the court addressed issues of copyright preemption and circumvention. Plaintiff Davidson & Associates (referred to by its dba "Blizzard") developed computer games that could be played in an online multi-player manner when in "Battle.net mode," using Blizzard's Battle.net servers. To prevent infringing copies of Blizzard games from being played at Battle.net, purchasers of authentic copies were required to enter a "CD Key" that was printed on a sticker attached to the product packaging. Based on this code, the games initiated an authentication sequence or "secret handshake" with the Battle.net server before online gaming was permitted.

The outside packaging of nearly all Blizzard games displayed a notice that the game and service were subject to an end-user license agreement (EULA) and Terms of Use (TOU). Before installing a copy of a Blizzard game, a purchaser was required to select and click on a button marked "I agree," manifesting acceptance of the EULA and TOU. The EULA prohibited reverse engineering and the TOU barred users from engaging in emulation or from hosting or providing "matchmaking" services for Blizzard games.

Defendants developed, apparently on a non-commercial basis, an alternative online gaming environment for the Blizzard games, designed to emulate Battle.net but hosted on defendants' own server at bnetd.org. In order to do so, defendants (who had previously agreed to the EULA and TOU) reverse engineered Blizzard's games to learn how to use their protocol language, modified the computer file that directed players to Battle.net, and created the Battle.net-emulating bnetd.org server on which they provided matchmaking services for multi-player game play. But unlike Battle.net, bnetd.org did not determine whether a CD Key was valid or already in use before allowing access to Battle.net mode, and therefore did not prevent infringing copies of Blizzard games from being played online.

Blizzard sued for copyright and trademark infringement, breach of contract and unlawful circumvention. The copyright and trademark claims were resolved pursuant to a consent decree and permanent injunction whereby the defendants would transfer the bnetd.org domain name to Blizzard, would be enjoined from participating in future efforts to develop any emulators for Blizzard games, and would face no liability for monetary relief on any claim. The existence of the consent decree is mentioned in the district court and appellate opinions, but its terms are not recited and seem to play no role in the analysis.

Blizzard won summary judgment on the remaining claims, for breach of the EULA and TOU and for unlawful circumvention. The Eighth Circuit affirmed in an opinion so confusing and cryptic at points as to border on incoherence. Below, we summarize the outcomes and attempt to extract possible "holdings" from the decision.

Regarding the EULA – TOU contract claims.

Davidson stands for two propositions:

- EULAs and TOUs are enforceable contracts when assent is manifested through click-on license agreements.
- A contractual prohibition against reverse engineering is enforceable against the defense that reverse engineering contract provisions are "preempted" by the Copyright Act.

Regarding the DMCA Circumvention claim.

In a particularly confusing part of its opinion, the Eight Circuit determined that the bnetd.org server and emulator were a circumventing technology under 17 U.S.C. § 1201(a)(2) (which deals with access controls), and that the reverse engineering defense under § 1201(f) did not apply.

The court does not state what was being protected from unauthorized access by the technological protection measure, and the prima facie violation is not clear. The totality of the Eighth Circuit's explanation: "The bnetd.org emulator had limited commercial purpose because its sole purpose was to avoid the limitations of Battle.net. There is no genuine issue of material fact that Appellants designed and developed the bnetd.org server and emulator for the purpose of circumventing Blizzard's technological measures controlling access to Battle.net and the Blizzard games."

CD Key, the secret handshake and the protocols that prevented unauthorized access to Battle.net appear to constitute effective technological measures entitled to protection against circumvention. But they prevented unauthorized access to Battle.net, and the defendants did not bypass these measures to engage in or facilitate unauthorized (or any other) access to Battle.net. Rather, they afforded access to their own, emulating server, which offered comparable functionality. Similarly, as far as can be discerned from the court's opinion, the CD Key does not control access to the Blizzard game itself (as opposed to controlling a game's access to a server for purposes of multi-player play), and it does not appear that defendants circumvented an access control (if any there be) for the game. Interpreting broadly, and without the benefit of much analysis by the court, the Eighth Circuit was arguably holding:

- When a party provides access to a non-infringing, emulating server as an alternative to a server protected by the publisher's access controls, this constitutes "circumvention" of the access controls employed by the publisher's server.

The reverse engineering defense.

The court rebuffed defendants' "reverse engineering" defense under § 1201(f)(1). This section exempts a circumventor from liability when the circumvention's "sole purpose [is] identifying and analyzing those elements of [a] program that are necessary to achieve interoperability of an independently created computer program...to the extent any such acts of identification do not constitute [copyright] infringement under this title [Title 17]."

The wording of the statute is confusing, and it is not clear how "acts of identification" of elements necessary for interoperability could ever themselves constitute copyright infringement. Interestingly, when the Eighth Circuit summarized the requirements of the statute, it stated the condition as that "the *alleged circumvention* did not constitute infringement."[6]

Presumably, this was the basis of the court's rejection of the reverse engineering defense: Immediately after reciting the requirements of § 1201(f)(1), the Eighth Circuit simply stated: "Appellants' circumvention in this case constitutes infringement." By way of explanation, the court alluded to the fact that defendants' bnetd.org server allowed Blizzard game users to access Battle.net mode features and to play with other gamers on the bnetd.org server regardless of whether they had a valid CD key, with the result that unauthorized copies of Blizzard games could be and were freely played on bnetd.org servers.

But what was the infringement? Making a server available for the exchange of game data among Blizzard players (some of whom use infringing copies) would not appear to constitute direct copyright infringement by defendants. Neither would such actions appear to constitute contributory infringement. That requires proof of (1) an underlying direct infringement, to which (2) the defendant materially contributes (3) with knowledge of the direct infringement. In *Davidson,* the defendants knew that unauthorized and presumptively infringing copies had been made and that they were being used in conjunction with bnetd.org. But since defendants did not apparently participate, directly or otherwise, in the creation of any "pirated" copies of Blizzard games, their actions would not ordinarily be said to "materially contribute" to an infringing act. Although the Eighth Circuit does not trouble to play out the analysis, the following theories might explain the outcome:

- Circumvention defendants are not entitled to the reverse engineering defense of § 1201(f) if their reverse engineering allows a direct infringer to use his infringing copy interoperably with the defendants' independently created program.
- The "non-infringement" requirement of the § 1201(f)(1) defense is violated by acts that would make a party secondarily liable as well as by direct infringement. Each time an unauthorized copy of a Blizzard

SEE *Circuit Court* PAGE 15

> game is launched, a new infringing copy is made in the RAM of the infringer's computer. The defendants—by offering an otherwise unavailable service to the infringer at that time—provided an incentive for the creation of the infringing RAM copy and facilitated the Battle.net mode use of that copy. Hence, they should be deemed (contributory) infringers.

The first point is suggestive of "accessory after the fact" liability, not secondary liability under copyright. The second point evokes the new "inducement of infringement" doctrine, but without meeting the high standard for copyright inducement set forth by the Supreme Court in *MGM v. Grokster.*

CONCLUSION

Although the reasoning in neither *StorageTek* nor *Davidson* is especially satisfying, the outcomes are clear enough. In *StorageTek,* the Federal Circuit, treating the interpretation of § 117(c) as an issue of first impression, stretched the statute to allow third party use of maintenance programs, in purported furtherance of Congress's pro-competition policy, at the expense of copyright holders. In *Davidson,* the Eighth Circuit expanded the sweep of the anti-circumvention provisions of the DMCA by treating "circumvention" broadly and by interpreting the reverse engineering defense narrowly, to the benefit of copyright holders who employ technological protection measures. Neither case is likely to be the last word on its subject. Meanwhile, however, these circuit court decisions cannot be ignored. ⊙

Mitchell Zimmerman is a partner in the Intellectual Property and Litigation Groups at Fenwick & West LLP, and Chair of its Copyright Group. He has represented Sun Microsystems, which recently acquired Storage Technology, the plaintiff in the first case discussed in this article.

Endnotes

1. 421 F.3d 1307 (Fed. Cir. Aug. 24, 2005).
2. 422 F.3d 630 (8th Cir. Sept. 1, 2005).
3. 2005 U.S.App.Lexis 27246 (Dec. 14, 2005).
4. Pet. for Rehearing at 10.
5. 381 F.3d 1178.
6. 2005 U.S. App. Lexis 18973 at *30, emphasis added.