The John Marshall Journal of Information Technology & Privacy Law

Volume 25
Issue 4 *Journal of Computer & Information Law - Symposium*

Article 7

2008

Access To Computer Programs Under The DMCA, 25 J. Marshall J. Computer & Info. L. 641 (2008)

Dennis S. Karjala

ACCESS TO COMPUTER PROGRAMS UNDER THE DMCA

DENNIS S. KARJALA*

I. INTRODUCTION

Computer programs are the quintessential example of the merger of information and technology. Source code is a descriptive program for the operations a computer should carry out, and falls squarely within the class of "literary work" under the Copyright Act.[1] Object code is the direct result of compiling this literary-work source code into a binary representation. We usually think of this binary representation as sequences of binary numbers (zeroes and ones). Printed out on paper, this binary representation would still constitute a set of numerical symbols, thus formally qualifying as a literary work. There is rarely any reason for a consumer to print out a binary representation of object code, however, in electronic form, object code is comprised simply of physical signals that directly cause electrical currents to flow in a computer in a way that humans can interpret as "information processing."[2] That is, in elec-

* Dennis S. Karjala has a B.S.E. from Princeton University and holds a Ph.D. in electrical engineering from the University of Illinois. He received his J.D. from the University of California, Berkeley. Professor Karjala joined the College of Law at Arizona State University in January 1978 as Associate Professor, after five years of private practice in San Francisco. He has been a Professor of Law since the fall of 1981 and currently holds the Jack E. Brown Chair. His teaching and research are primarily in the area of intellectual property law, especially copyright and the application of intellectual property law to digital technologies. Other areas of teaching and earlier writing include corporate and securities law and federal income taxation.

1. 17 U.S.C. § 101 (2006). "Literary works" are works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied.

2. Dennis S. Karjala, *Coherent Theory For The Copyright Protection Of Computer Software and Recent Judicial Interpretations*, 66 U. CIN. L. REV. 53, 66 (1997). [hereinafter *A Coherent Theory*]. *See also* Dennis S. Karjala, *Copyright, Computer Software, and the New Protectionism*, 28 JURIMETRICS J. 33, 36-38 (1987) (explaining that object code in electronic form cannot be "read" by human beings at all, because it exists as distinct physical states, such as a high or low voltage.) We can represent physical object code by 0's and 1's and write it out on paper or in a memory "dump," but the zeroes and ones cannot make a computer, or anything else, do anything until they are retranslated into physical signals.

tronic-form, object code is a physical part of a physical machine. The physical electronics that cause these current flows constitute technology under anyone's definition, and computer programs thus reflect a complete merger of information and technology.

What does it mean to "access" information in a copyright-protected work? Access to traditional works is available in many ways. Consumers can buy copies of the traditional works, they can browse copies in public places like bookstores and libraries, and they can view copies and public performances of works in places like movie theaters. Such traditional copyright subject matter is nonfunctional, in that it serves no utilitarian function other than to convey information or portray an appearance,[3] access to copies of a work gives access to the work itself. This includes the power to make further copies.

Computer programs are different. What most consumers want from a computer program is the functionality of the program and not the "literary work" that is the basis for its copyright protection, or the "set of statements or instructions"[4] comprising the program code. For example, people buy a video game for the purpose of using the code to operate a computer so that they can play the game, and not for the purpose of reading the code. Direct human access to source code is useless to most consumers. Direct access to electronic-form object code is also useless unless they have a computer on which to run the software. If they have a computer that can run the software, they access the functionality of the program when they do so, but they do not access, in any meaningful sense, the code that is directing the electronic flow inside the machine.

Access to program code, especially object code, is of important copyright significance. Access to object code allows the kind of cheap and fast literal copying that justifies copyright protection for such a functional work in the first place.[5] For copyright purposes, therefore, we must dis-

---

Id. *See also* Dennis S. Karjala, *Copyright Protection of Computer Program Structure*, 64 BROOKLYN L. REV. 519, 519 (1998).

3. 17 U.S.C. § 101 (2006) (defining a "useful article" as one "having an intrinsic utilitarian function that is not merely to portray the appearance of the article or to convey information."). The Act's definition of "useful article" captures (perhaps fortuitously) much of the traditional distinction between patent and copyright subject matter and therefore serves as a starting point for a coherent analysis of why we continue to have two major intellectual property paradigms instead of merging patent and copyright together. *Id.* Dennis S. Karjala, *Distinguishing Patent and Copyright Subject Matter*, 35 CONN. L. REV. 439, 448-58 (2003) [hereinafter *Distinguishing Patent and Copyright Subject Matter*].

4. 17 U.S.C. § 101 (defining "computer program").

5. *See, e.g.*, Karjala, *Distinguishing Patent and Copyright Subject Matter, supra* note 3 at 448-58. The policy bases for including program code (a functional work) under copyright. Functionality, properly defined, is the boundary between traditional patent and copyright subject matter. Computer programs differ from most other functional subject matter in that it is often easy to copy and distribute programs in competition with their

tinguish between access to computer program code and access to the functionality of that program code. Unless that functionality itself represents some independently copyright-protectable expression, such as a video game character, writing independent program code to achieve the same function is not copyright infringement.[6]

II. ACCESS AND THE DIGITAL MILLENNIUM COPYRIGHT ACT

Section 1201(a)(1) of the Digital Millennium Copyright Act ("DMCA") prohibits circumventing a technological measure that effectively controls access to a copyright-protected work, while 1201(a)(2) prohibits trafficking in devices that allow such circumvention.[7] The key word here is "access." In the case of a computer program, does the statute mean access to the program code or access to the program's function-

---

authors essentially without any investment in production facilities. Because patent law protects only non-obvious innovation, most computer programs do not qualify for patent protection. Without legal prohibitions against direct, literal copying of electronic-form object code, there is a serious risk of market failure. *Id.* *See also* Karjala, *A Coherent Theory, supra* note 2, at 66-72. Because patent alone would leave a risk of market failure, some sort of anti-literal-copying regime is at least plausible. *Id.* Society probably would have been better off with a sui generis program-protection statute that could expressly take program functionality into account in setting, and limiting, the scope and duration of protection. *Id.* *See also,* Pamela Samuelson, *Creating a New Kind of Intellectual Property: Applying the Lessons of the Chip Law to Computer Programs*, 70 MINN. L. REV. 471 (1985) (explaining that copyright does, however, at least address the market failure problem by prohibiting copying of code, although it leaves open arguments over the scope of protection for both programs and user interfaces). *Compare* Whelan Assoc. v. Jaslow Dental Lab., 797 F.2d 1222 (3d Cir. 1986) (broadly protecting so-called "structure, sequence, and organization" or SSO of a program), *with* Computer Assoc. Int'l v. Altai, 982 F.2d 693 (2d Cir. 1992) (rejecting protection for SSO or other non-literal elements dictated by efficiency or external demands), *and* Digital Commc'n Ass'n. v. Softknlone Distrib. Corp., 659 F. Supp. 449 (N.D. Ga. 1987) (broadly protecting user interfaces as an element of the program) *with* Lotus Dev. Corp. v. Borland Int'l, Inc., 49 F.3d 807, 815 (1st Cir. 1995) (denying protection to a menu command hierarchy as a "method of operation"). *See also* Dennis S. Karjala, *Copyright Protection of Operating Software, Copyright Misuse, and Antitrust*, 9 CORN. J. L. & PUB. POL. 161 (1999) (explaining that network effects imply that protecting operating software under copyright will lead to single firm dominance).

6. *See Lotus Dev. Corp.*, 49 F.3d at 815 , *aff'd by an equally divided Court* 516 U.S. 233 (1996) (holding that independently written code generating the same "menu command hierarchy" does not infringe. Indeed, even copying the code for the purpose of writing an independent program that compatibly performs the same function in competition with the original is a fair use); Sony Comp. Entm't v. Connectix, 203 F.3d 596, 599-01 (9th Cir. 2000) (involving the reverse engineering of a game console's operating system for the purpose of creating an independently coded but compatible platform).

7. 17 U.S.C. § 1201(a)(1)-(2). Section 1201(b)(1) prohibits trafficking in devices that allow circumvention of technological measures that protect rights of copyright owners, such as the exclusive right to reproduce the work. For short, this can be referred to as a "copy circumvention" provision, in contrast to the "access circumvention" provisions of 1201(a)(1) & (2).

ality? As a policy matter, we must recognize that the reason for including functional computer code under the protective umbrella of copyright is to reduce the potential for market failure that would otherwise arise if the copying of code were unrestricted by law.[8] If code can be written independently to perform the same function as a protected computer program, free competition in the market should be the arbiter of things like price and quality. This is unless, of course, the functionality in a particular case is protected by patent. Somewhat surprisingly, most of the courts that interpreted the DMCA's access provisions have intuitively adopted this perspective. As a result, the DMCA may not have the negative impact on access, at least to computer software, that many feared when the statute was passed.

Movies on DVD supply a concrete example of the need to distinguish between access to the protected work and access to the functionality of a computer program. At issue in *Universal City Studios, Inc. v. Reimerdes*[9] was access to traditional audiovisual works, namely, motion pictures that were embedded on DVDs. The binary code representing a movie was encrypted by a Content Scrambling System ("CSS"), aimed at allowing the movie to be played only on devices equipped with licensed descramblers. Licensed descramblers of the CSS encryption system allowed playing the films, but not copying them. The descramblers would not even allow the owners of legally made copies of the DVD to play them, if the DVD included codes aimed at limiting the geographical locations where the film could be played.

This is a classic situation for application of the access-regulation provisions of the DMCA. The danger was that the DeCSS system made freely available on defendants' website, together with a freely available compression program, could allow copying and further distribution of films. These films are copyright-protected audiovisual works whose copyright is independent of any computer code embodying the work in a tangible medium. The copied films were no longer access-protected and could be played on any DVD playback device. "Access" as such, was not an issue in the case; rather the defendants unsuccessfully argued that the CSS system did not "effectively" control access and therefore, DeCSS did not circumvent an access-protection measure covered by the DMCA.

An interesting issue not directly raised in *Universal City Studios* is how the DMCA would apply if the decryption system circumvents not the entire protection system, but only the region or country codes designed to restrict playback to specific regions or countries. If an owner of a DVD country coded for Japan circumvents the country code and plays the film

8. *See supra* note 5.

9. Universal City Studios v. Reimerdes, 82 F. Supp.2d 211 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

in the U.S., has there been a violation of the DMCA, and would selling a device that allows circumvention of the country code violate the anti-trafficking provisions? Use of such a device does not allow any of the evils that the DMCA was designed to reduce. The DMCA was not designed to give copyright owners even *greater* rights.[10] Book publishers historically never had the right to prohibit the reading in the U.S. of books acquired in Japan. Now that digital technologies potentially allow more control over uses than was possible in the analog era, we should be careful before expanding copyright owners' rights without thinking about whether there is a problem that needs a remedy. What goals of *copyright law* promote the power of an audiovisual work copyright owner to control where a legal copy of the film is viewed? Copyright law gives the copyright owner a limited market advantage through the exclusive rights of reproduction, adaptation into derivative works, and public distribution, performance, and display. When these exclusive rights are not infringed, a copyright owner's business model is relegated to the market to try to control uses of the work. If the copyright owner believes it to be advantageous to insert country codes on DVD's and can do so with technology, we may well say that he is free to try, but there is no reason for copyright law to come to his assistance in enforcing this aspect of his business model. Viewing a Japanese film on a machine coded for the U.S. does not present any more danger of actual copyright infringement (violating exclusive rights of reproduction, distribution, or public performance) than it does when viewed on a machine coded for Japan. In other words, the circumvention in this case only gives access to the functionality of the encoded signals in the playback device. It does not give any more access to those signals than the viewer had prior to the circumvention.

Davidson & Associates. v. Jung,[11] is one of the few United States appellate court decisions to show the distinction between the protected program code and its unprotected functionality, all wrong in the context of the DMCA. In this case, the copyright owner sold video games that customers purchased on CD-ROM and installed on their computers. While customers could form their own private networks to play against each other, the copyright owner, doing business under the name Blizzard Entertainment, Inc., offered a free service that allowed users anywhere on the Internet to play each other through a Blizzard-operated server called "Battle.net." The service was available to purchasers of Blizzard games through an authentication sequence ("secret handshake") based

10. *See* 17 U.S.C.A. § 1201(c)(1) (2006): "Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."

11. Davidson & Assoc., dba Blizzard Entm't v. Jung, 422 F.3d 630 (8th Cir. 2005).

on a CD key printed on a sticker attached to the CD-ROM purchased by the user. Software-savvy users unsatisfied with the quality of the Battle.net service managed to reverse engineer the Battle.net software and set up their own server, called bnetd.org. Owners of Blizzard game CD-ROM's could use this server to play against each other free of whatever restrictions were imposed by Battle.net. This included the freedom from access denials for users who could not pass the authentication sequence (in some cases, almost certainly, because such users had pirated copies of the game software).

While there were important issues in the case of both state-law preemption[12] and a reverse engineering defense under section 1201(f)[13] of

12. *Id.* at 634-35. Users agreed to both an End User License Agreement (EULA) with respect to the CD-ROM software and a Terms of Use (TOU) agreement with respect to the Battle.net service, both of which prohibited reverse engineering. Defendants argued that state enforcement of this term under contract law conflicted with federal copyright's allowance of certain kinds of reverse engineering as a fair use. Relying upon *Bowers v. Baystate Techs, Inc.*, 320 F.3d 1317, 1325-26 (Fed. Cir. 2003), which also involved a shrink wrap license, the *Davidson* court rejected the preemption argument, holding that private parties are free to contract away their rights under copyright law. 422 F.3d at 639. By following *Bowers* and failing to recognize a distinction between privately negotiated contracts and shrinkwrap or clickwrap licenses, which are binding on essentially anyone who acquires the software with notice, the court allows state law nominally called "contract" to become binding on the world. Carried to its logical extreme, this reasoning would allow elimination of all the users rights of federal copyright pursuant to state law of "contract." *See* Dennis S. Karjala, *Federal Preemption of Shrinkwrap and On-Line Licenses*, 22 U. DAYTON L. REV. 511 (1997).

13. 17 U.S.C.A. § 1201 (f)(1):

> [A] person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

The statute predicates this exemption on a lawful "right to use a copy of a computer program." In this case, the reverse engineered computer program is the Battle.net software. If the defendants lost their right to use that software by breaching the EULA and TOU prohibitions on reverse engineering, one can argue that they were no longer using the Battle.net software "lawfully," whether or not such use in breach of the contract amounted to copyright infringement. Of course, if this reasoning is accepted, the entire reverse engineering exemption could be rendered nugatory by drafting shrink wrap licenses that make further use of the program "unlawful" as soon as any effort at reverse engineering is attempted. A better interpretation of someone who has "lawfully obtained the right to use a copy of a computer program" is that it refers to someone who has complied with all the legal requirements for acquiring the copy or use of the copy, such as paying for the CD-ROM or the monthly service fee. While it was probably not for this reason (i.e., that the "lawfully obtained the right to use a copy" language is problematic for finding a DMCA violation on these facts), the Eighth Circuit in *Davidson* took a different tack. It simply concluded that the defendants' circumvention constituted copyright infringement. 422 F.3d at 642. The

the DMCA, the important point for present purposes is the court's handling of the access issue under section 1201(a). We may assume with respect to section 1201(a)(1) that there was some sort of circumvention that allowed access to the functionality of the Battle.net software.[14] The point is that the defendants never accessed the Battle.net code, and they certainly never had an opportunity to copy that code. Accessing the functionality of a program is one of the classic ways of reverse engineering, and it often does not involve a copyright infringement, except in the technical sense that a copy must be reproduced in RAM before the program will function and its functionality can be observed. The defendants' activity did not render the Battle.net code available even to the defendants, let alone to anyone else. The defendants were trying to build a competing platform on which users of Blizzard game software could play their games. Those players did not circumvent *anything* when they used the bnetd.org platform, so that platform cannot be a device that permits circumvention of a technological measure under section 1201(a)(2). It is true that even owners of pirated copies of Blizzard games could play them on bnetd.org, but that is true for any compatible platform software. If one wrote a non-infringing but compatible copy of the Windows operating system, a pirated copy of an application will run just as well as a

---

"circumvention" was apparently getting around the "secret handshake" to access to the functionality of the Battle.net software, which is what defendants were trying to reverse engineer, but there is no indication that defendants' access of Battle.net was pursuant to anything other than a legitimate CD key. The bnetd.org emulator of Battle.net did not determine whether someone playing the game had a valid copy of the Blizzard program. (It could never make such a determination without breaking Blizzard's "secret handshake" formula.) Therefore, *users* of bnetd.org could circumvent the need to authenticate. But that has nothing to do with what the *defendants* did in reverse engineering the Battle.net software, nor did the users circumvent anything when they accessed bnetd.org, which is an independently written and, we may assume, non-infringing emulator of Battle.net. The whole point of § 1201(f) is to *permit* circumventions for purposes of achieving interoperability of an independently created program with other programs. Here, the independently created program was bnetd.org. It was to be interoperable with "other programs," namely, the Blizzard games that could be played through Battle.net. Therefore, the § 1201(f) exemption should have been available. The Eighth Circuit never tells us exactly how the circumvention in question constituted copyright infringement, as opposed to breach of contract. Nonetheless, the ability of users to play their games without authentication was enough, for the Eighth Circuit, to deny the reverse-engineering exemption.

14. Davidson & Assoc., dba Blizzard Entm't, 422 F.3d at 636. The summary of the court's analysis of the reverse engineering activity: Defendants logged communications between Blizzard games and Battle.net. They used a "ripper" program to break apart Blizzard client files into component parts. They used the same ripper program to learn how to display ad files on bnetd.org in the same way as Battle.net. They even disassembled a Blizzard program in an effort to allow bnetd.org to protect the password that a user entered to play through Battle.net (which one would have thought would operate in the defendants' moral favor). They also used an unauthorized copy of a Blizzard program for testing purposes. That infringement, if it was one, seems separable from the basic reverse-engineering activity, as the defendants could easily have used an authorized copy for testing purposes.

legitimate copy. The DMCA was not meant to protect against piracy of this type, because it would mean that no one could try to develop compatible platforms, contrary to the evident purpose of section 1201(f) and the policies underlying the cases holding that reverse engineering for compatibility purposes is a fair use.[15]

The Eighth Circuit's decision in *Davidson* conflicts with an earlier and better reasoned decision of the Sixth Circuit in *Lexmark v. Static Control Components, Inc.*[16] This case also involved an authentication sequence, but between a printer toner cartridge and a printer. The defendant reverse engineered the authentication sequence to make refill cartridges compatible with the printer, without which they could not be reused. The plaintiff argued that its authentication sequence effectively controlled access to a work, namely the program controlling the printer, and that the defendant's reprogrammed cartridge circumvented that access restriction. The court correctly recognized that the authentication sequence did not control access to the printer program because the program code was readily available for reading directly from the printer's memory.[17] The court expressly noted that access in the sense of "ability to use the program" was blocked by the authentication sequence, but the relevant sense was "ability to obtain" a copy of the work or to make use of the literal elements of program code.[18] Thus, the *Lexmark* court clearly distinguished between access to the functionality of a computer program and access to the program code.

The Federal Circuit is consistent in its interpretation of "access" under the DMCA. Like *Lexmark*, the Federal Circuit in *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*[19] looked to the statutory structure and the legislative history to conclude that section 1201 only applies to "circumventions reasonably related to protected [copyright] rights."[20] This case involved a garage door opener that operated by radio communication between a hand-held remote control unit and the motor that opened the door. Plaintiff's design used "rolling codes" in the communication between the two devices, aimed at preventing a potential burglar from capturing a legitimate signal from the homeowner and using that same signal to open the door at a later time. The defendant sought to

15. Sony Computer Entertainment Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000) (holding that reverse engineering of game console software to build a compatible but competing console is a fair use); Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992), *amended by* Order and Amended Opinion, D.C. No. CV-91-3871-BAC, Jan. 6, 1993 (holding that reverse engineering of game software to permit the independent creation of new games compatible with a popular console is a fair use).

16. Lexmark Int'l v. Static Components, 387 F.3d 522 (6th Cir. 2004).

17. *Id.* at 546.

18. *Id.* at 547.

19. Chamberlain Group v. Skylink Technologies, 381 F.3d 1178 (Fed. Cir. 2004).

20. *Id.* at 1195.

offer a universal transmitter that would work with many different brands of garage door openers, including the plaintiff's. The defendant's device did not use the same rolling code technology. Rather, the device simulated the effect of the rolling codes by causing the motor program to resynchronize itself every time the device was used.[21] Plaintiff claimed that its rolling codes technology was a technological measure that controlled access to the motor program. The Federal Circuit, however, recognized that the homeowners who purchased the device were authorized to use the software embedded in it. The anti-circumvention provisions do not give new property rights but simply give copyright owners new ways to secure their existing rights.[22] Thus, there must be some connection or nexus between the circumvention and copyright.[23] If the circumvention does not relate to copyright rights, the DMCA could allow leveraging sales of physical devices into after-market monopolies.[24] Thus, while not using the exact words, *Chamberlain* too distinguishes between access to program functionality and access to program code. Only the code is protected by copyright, not the functionality. Purchasers of the program have the right to make use of its functionality. Indeed, there is no other reason for them to buy it.

Storage Technology Corporation. v. Custom Hardware Engineering & Consulting, Inc.,[25] expands the Federal Circuit's nexus requirement set forth in *Chamberlain*. The basic battle in this case was the familiar one between a special-purpose computer manufacturer and third-party repair and maintenance services. The plaintiff manufactured digital tape storage libraries accessible through a general Management Unit and a Control Unit attached to each library or "silo" containing the actual data tapes. The program code governing the operations of each Unit serves two distinct purposes. First, it causes the Units to act together to access and deliver the information requested by a user, through what is called "functional code." Second, when the Units are properly configured, the code causes the Control Unit to send out messages indicating the state of the system, in particular, error messages indicating both the existence and the location of a problem. The part of the program achieving this latter function is called "maintenance code." Both functional code and maintenance code are so intertwined that any boot of the system it causes both to be loaded into RAM. However, the license agreements between plaintiff and its customers explicitly excludes the

21. *Id.* at 1184-85.

22. *Id.* at 1193-94.

23. *Id.* at 1195, 1202.

24. *Id.* at 1201.

25. Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, 421 F.3d 1307 (Fed. Cir. 2005).

maintenance code from the license.[26]

Defendant in *Storage Technology* repaired and performed maintenance services on data libraries manufactured by plaintiff. Defendant did not use its own diagnostic software, but took advantage of error messages sent out by the maintenance code automatically loaded into RAM when the system was switched on. However, the Control Unit would not send error messages unless it was configured to do so, and plaintiff attempted to prevent unauthorized reconfigurations by means of a password protection scheme called "GetKey." Defendant first overcame "GetKey" by brute force. Defendant tried different passwords until one worked, allowing them to reconfigure the system. Subsequently, defendant found a means of mimicking a signal from the Management Unit to the Control Unit upon a reboot that reconfigured the Control Unit to send the error messages. The DMCA issue was whether this circumvention gave access to a copyright protected work.[27] The court relied on its nexus requirement in denying the DMCA claim, saying that there was no nexus between any possible infringement and the circumvention.[28] It should be clear that the circumvention in this case gave access to the functionality of the maintenance code, but it did not make that code any easier to copy than it already was. After the circumvention and reconfiguration of the Control Unit, Defendants took advantage of the functionality of the maintenance code by receiving and interpreting the error messages that were sent out. The defendants never looked at the maintenance code. Given the way the two program functions were intertwined Defendants may have had a hard time figuring out which parts were "maintenance" and which parts were "functional" in any event.

---

26. *Id.* at 1309-10.

27. *Id.* at 1307. Another important issue in the case was whether defendant's copying of the maintenance code upon reboot and use of that maintenance code after reboot was exempt from infringement claims by section 117(c). This section allows an owner to make a copy by activating a machine containing a lawful copy of a program solely for purpose of maintenance and repair, provided the copy is destroyed after the maintenance or repair is completed and that any program not necessary for the machine to be activated is not accessed or used. 17 U.S.C. § 117(c) (2006). The court concluded, on the facts before it, that the functional code and the maintenance code were so intertwined that simply turning on the machine caused both to be loaded into RAM. The maintenance code, therefore, *was* necessary for the machine to be activated, so the prohibition on use of programs not necessary for activation was wholly inactive. It also concluded that "maintenance," as opposed to "repair," can be an ongoing operation, so that the requirement to destroy the copies after maintenance is completed was met when the machine was turned off upon the expiration of the 3-year maintenance contract.

28. *Storage Tech. Corp.*, 421 F.3d at 1319.

III. CONCLUSION

With the exception of *Davidson*, we see that the DMCA "access" cases have resisted the temptation simply to treat a "bad" act, such as breach of contract, as a DMCA violation. Notwithstanding fears that the DMCA might lead to much broader copyright protection than that afforded by traditional copyright law, *Chamberlain*, *Lexmark*, and *Storage Tech* all take an explicitly narrow view of the reach of the DMCA. Other cases take a similarly narrow view of what constitutes "circumvention," holding that applying a validly issued user ID and password without authorization[29] and access in the usual way where the technological measure to deny access, does not function[30] as circumvention under the statute. Moreover, courts are getting increasingly explicit that uses of a work in violation of a license agreement rise to the level of copyright infringement only when those uses would infringe in the absence of any agreement at all.[31]

Under these decisions, the mere breach of a license agreement, such as a EULA, will not allow the copyright owner to leverage that breach into a copyright infringement or DMCA violation. This result makes sense. Copyright seeks to give the copyright owner power to control the market for copies of the *protected work* by granting the exclusive rights to reproduce the work, prepare derivative works based on it, or publicly distribute, perform, or display the work. Even these rights are limited by such doctrines as fair use and first sale. Copyright is not designed to protect any particular business model; even one the copyright owner believes will maximize income by controlling the use of copies. Unless one of the exclusive rights of copyright is threatened, the copyright owner is back in the world of competition and should look to the legal regimes in that world to implement any given business model.

---

29. Egilman v. Keller & Heckman, LLP, 401 F. Supp.2d 105, 114 (D.D.C. 2005); I.M.S. Inquiry Mgmt. Sys. v. Berkshire Info. Sys., 307 F. Supp.2d 521, 530-33 (S.D.N.Y. 2004).

30. Healthcare Advocates v. Harding, 497 F. Supp. 2d 627, 645-46 (E.D. Pa. 2007).

31. *E.g., Storage Tech. Corp.*, 421 F.3d at 1316; *Jacobsen v. Katzer*, No. C 06-01905 JSW (N.D. Cal. 2007).