PRESERVING COMPETITION FOR COMPUTER MAINTENANCE IN THE DMCA ERA: 17 U.S.C. § 117(C) AND § 1201(A)(1) AFTER *STORAGETEK*

By Alan Galloway

During the early 1990s, computer equipment manufacturers wielded copyright law as a sword against independent service organizations (ISOs) to dominate the market for computer repair and maintenance.[1] Industry licensing practices and copyright restrictions on RAM copies of computer programs left ISOs unable to even turn on computer hardware for repair without infringing copyright. In 1998, after manufacturers had won several infringement actions against ISOs,[2] Congress passed the Computer Maintenance Competition Assurance Act (CMCAA) to restore free competition in the computer service industry.[3] The CMCAA created section 117(c) of the Copyright Act—a safe harbor declaring that software copies made by activating a machine for repair or maintenance are noninfringing, subject to certain conditions.[4] Yet, in the same bill Congress enacted section 1201 of the Digital Millennium Copyright Act (DMCA), which created liability for the circumvention of technology protection measures (TPMs) restricting access to copyrighted works.[5] This raised the possibili-

1. *See, e.g.*, DSC Commc'ns. Corp. v. DGI Techs., 81 F.3d 597, 601 (5th Cir. 1996) ("DGI may well prevail on the defense of copyright misuse, because DSC seems to be attempting to use its copyright to obtain a patent-like monopoly over unpatented microprocessor cards"); MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 517-19 (9th Cir. 1993) (holding that ISO infringed manufacturer's software copyright by turning on computer for repair); CSU Holdings v. Xerox, 910 F. Supp. 1537, 1541-46 (D. Kan. 1995) (granting preliminary injunction against ISO that asserted manufacturer was misusing copyright to perpetuate antitrust violations); Advanced Computer Servs. of Mich., Inc. v. MAI Sys. Corp., 845 F. Supp. 356, 363-71 (E.D. Va. 1994) (holding that ISO infringed copyright of manufacturer controlling 90% of the repair market and rejecting ISO's antitrust claims).

2. *See Peak*, 991 F.2d at 517-19 (holding that an ISO infringed); *Advanced Computer Servs.*, 845 F. Supp at 363-71 (holding that ISO infringed); *CSU Holdings*, 910 F. Supp. at 1541-46 (granting preliminary injunction against ISO). *But see DGI*, 81 F.3d at 601 (denying preliminary injunction against ISO).

3. Computer Maintenance Competition Assurance Act (CMCAA), Pub. L. 105-304 § 302, 112 Stat. 2860, 2886-87 (1998) (codified at 17 U.S.C. § 117 (2000)); *see* H.R. REP. NO. 105-551, pt. 1, at 27 (1998) (discussing the goals of the amendments).

4. CMCAA, Pub. L. 105-304 § 302, 112 Stat. 2860, 2886-87 (1998) (codified at 17 U.S.C. § 117 (2000)).

5. The CMCAA was enacted as Title III of the Digital Millennium Copyright Act (DMCA) on October 28, 1998. The DMCA included the CMCAA, the WIPO Copyright

ty that, the CMCAA notwithstanding, manufacturers could use TPMs backed by DMCA liability to lock ISOs out of the market for maintenance.[6]

Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.[7] was the first appellate construal of the CMCAA,[8] clarifying both the scope of maintenance activities protected and the conditions for that protection.[9] Moreover, it was the first appellate decision to address whether maintenance activity protected by the safe harbor can nonetheless trigger liability under the DMCA's anti-circumvention provision, 17 U.S.C. § 1201(a)(1).[10] Finally, it clarified a critical intersection of contract law and copyright law by limiting the circumstances when breaches of software licenses give rise to copyright liability.[11]

In *StorageTek*, the Court of Appeals for the Federal Circuit vacated a preliminary injunction against an ISO that triggered RAM copies of software, circumvented a TPM, and made use of restrictively licensed software during a three-year maintenance contract.[12] The court interpreted § 117(c)'s safe harbor to cover long-term maintenance and the use of software that was not functionally necessary to activate the equipment.[13] The court held that the DMCA anti-circumvention provision, § 1201(a)(1)(A), creates no separate enforceable right where defendant's conduct neither constitutes nor facilitates infringement (and in particular, when the conduct falls within the § 117(c) safe harbor).[14] Finally, it cau-

---

and Performances and Phonograms Treaties Implementation Act of 1998, the Online Copyright Infringement Liability Limitation, and the Vessel Hull Design Protection Act, as well as miscellaneous provisions affecting small webcasters. Digital Millennium Copyright Act, Pub. L. 105-304, 112 Stat. 2860 (1998).

6. *See* Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095, 1096-97, 1140 (2003) (arguing that the anticompetitive potential of TPMs requires an equitable doctrine of anticircumvention misuse, in order to prohibit anticompetitive practices); *see also* Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of "Lock-Out" Programs*, 68 S. CALIF. L. REV. 1091, 1096-97 (1995) (arguing that technological "lock-out" measures merit copyright protection, but have potential for misuse when combined with license terms).

7. Storage Tech. Corp. v. Custom Hardware Eng'g. & Consulting, Inc. (*StorageTek II*), 421 F.3d 1307 (Fed. Cir. 2005), *further opinion on denial of reh'g*, 431 F.3d 1374 (Fed. Cir. 2005).

8. *Id.* at 1311.

9. *See id.* at 1312-15.

10. *See id.* at 1318.

11. *See id.* at 1316.

12. *Id.* at 1310, 1321.

13. *See id.* at 1313-14; Storage Tech. Corp. v. Custom Hardware Eng'g. & Consulting, Inc. (*StorageTek III*), 431 F.3d 1374, 1376 (Fed. Cir. 2005).

14. *StorageTek II*, 421 F.3d at 1318-19.

tioned that actions in breach of software licenses do not create copyright liability unless those actions violate the exclusive rights of section 106 of the Copyright Act.[15]

StorageTek preserves the spirit of the CMCAA by construing a robust § 117(c) safe harbor. The Federal Circuit's analysis suggests a coherent, restrained approach to the use of copyright law in the context of computer equipment manufacturers and ISOs competing in the market for hardware repair and maintenance. This approach disentangles copyright law from claims of anticompetitive conduct, from circumvention of TPMs that do not guard the exclusive rights of copyright, and from the *use* of software (as opposed to the copying or distribution of software) beyond the scope of a license. By curtailing the role of copyright law (and the availability of copyright remedies) in disputes that do not center on the traditional exclusive rights, this approach respects the CMCAA's goal of restoring the competitive balance inadvertently upset by the rise of digital copyright. The Federal Circuit's approach prevents hardware manufacturers from wielding copyright law as a sword against the ISOs responsible for maintaining their equipment, but also prevents use of the safe harbor as an absolute shield against license violations, trade secret misappropriation, or unfair competition.

Part I of this Note considers the legal background of both the CMCAA's safe harbor for maintenance, 17 U.S.C. § 117(c), and the DMCA's anti-circumvention provision, 17 U.S.C. § 1201(a)(1). Part II provides the factual record that gave rise to the claims and the district court proceedings in *StorageTek*. Part III examines the Federal Circuit's key holdings with respect to the § 117(c) safe harbor, the § 1201(a)(1) anti-circumvention provision, and licensing issues—arguing that the decision exhibits generally sound reasoning, preserves the CMCAA safe harbor, and sensibly limits copyright liability and remedies to disputes that center on conduct that tends to infringe the exclusive rights defined in 17 U.S.C. § 106. Part IV concludes that this decision is a positive development for both for copyright law and the computer service market.

I. LEGAL BACKGROUND

This Part provides the legal background of both the CMCAA's safe-harbor for repair and maintenance and the DMCA's § 1201(a)(1) anti-circumvention provision—the two provisions of copyright law at the center of *StorageTek*. Section I.A traces the origins of the obstacles to compe-

15. *Id.* at 1316.

tition in the computer service market that the CMCAA was enacted to remove. Section I.B surveys the various roles that TPMs play and the opposing views on how the DMCA reinforces the roles of TPMs.

A. The CMCAA's Safe Harbor for Computer Service: 17 U.S.C. § 117(c)

This Section explains how the competitive landscape for ISOs vying with computer manufacturers for service contracts was distorted by three elements—(1) copyright protection for computer software, (2) software licensing practices, and (3) court holdings that copyright encompasses RAM copies of software—such that ISOs could not even turn on equipment without infringing a manufacturer's copyright. This provoked Congress to enact the CMCAA, with its § 117(c) safe harbor, to restore fair competition for computer repair and maintenance.[16]

In 1980, Congress embraced copyright protection for software as a literary work. Although the Copyright Act of 1976 included a definition of "literary works" broad enough to encompass software code,[17] its original section 117 specified that any software protections under previous law were unchanged—preserving the status quo as Congress awaited the report of the National Commission on New Technological Uses of Copyrighted Works (CONTU).[18] Congress had established CONTU in 1974 to study the reproduction, use, and creation of copyrighted works in conjunction with automatic systems.[19] In 1978, CONTU recommended that both source and object code should be protected by copyright as literary works,

16. *See* S. REP. NO. 105-190, at 21 (1998). The Senate Report stated that the new section would "ensure that independent service organizations do not inadvertently become liable for copyright infringement merely because they have turned on a machine in order to service its hardware components." *Id.* at 21 (1998).

17. *See* 17 U.S.C. § 101 (Supp. II 1978). "'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." *Id.*

18. *See* 17 U.S.C. § 117 (Supp. II 1978). The House Report reveals Congressional uncertainty, upon enacting the Copyright Act of 1976, regarding both whether copyright already protected software and whether it ought to do so. The report noted that "the problems are not sufficiently developed for a definitive legislative solution," and stated that CONTU would "recommend definitive copyright provisions to deal with the situation." H.R. REP. NO. 94-1476, at 116 (1976), *as reprinted in* 1976 U.S.C.C.A.N 5659, 5731 (1976).

19. FINAL REPORT OF THE NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS 1 (July 31, 1978) [hereinafter "CONTU REPORT"], *available at* http://digital-law-online.info/CONTU/PDF.

subject to certain limitations.[20] Congress embraced this recommendation in 1980 by simply adding computer programs to the definitions listed in 17 U.S.C. § 101 and rewriting § 117 to permit the owner of a program copy to make (or authorize) copies necessary to utilize or archive the software.[21]

In 1993, in *MAI Systems Corp. v. Peak Computer, Inc.*,[22] the Ninth Circuit held that (a) random access memory (RAM) is a tangible medium of expression, and consequently, that (b) the § 106 reproduction right encompasses loading software from a storage device (e.g., a disk) into RAM.[23] Other courts followed this holding, creating obstacles to competition in the computer repair industry.[24] *Peak* illustrates the resulting problem for ISOs. Peak was an ISO hired to repair equipment manufactured by MAI.[25] Whenever Peak turned on the equipment to service it, the equipment automatically loaded a copy of MAI's software into RAM.[26] Based on this copying, the Ninth Circuit held that Peak infringed MAI's copyright.[27]

---

20. *Id.* at 1, 12-15.

21. *See* Copyright Act Amendments of December 12, 1980, Pub. L. No. 96-517, 94 Stat. 3015, 3028 (codified as amended at 17 U.S.C. § 101 and § 117 regarding computer programs (Supp. IV 1980)). The language of § 117, as enacted in 1980, allowed owners of programs to copy programs as an "essential step" in the utilization of the program, and to make and keep backup ("archival") copies of programs they owned. 17 U.S.C. § 117 (Supp. IV 1980). The CONTU report had recommended language identical but for the substitution of "rightful possessor" for "owner." *Compare* CONTU REPORT, *supra* note 19, at 12, *with* 17 U.S.C. § 117 (Supp. IV 1980).

22. MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 519 (9th Cir. 1993).

23. Section 106 of the Copyright Act gives owners of copyrights in literary works five exclusive rights: reproduction, preparation of derivative works, distribution, public performance, and public display. 17 U.S.C. § 106 (2000).

24. *See, e.g.*, Stenograph L.L.C. v. Bossard Assocs., 144 F.3d 96, 101 (D.C. Cir. 1998) (citing *Peak* for the proposition that loading into RAM creates a "copy"); DSC Commc'ns. Corp. v. DGI Techs., 81 F.3d 597, 600 (5th Cir. 1996) (citing *Peak* for the proposition that a copy is made when software is loaded into RAM); NLFC, Inc. v. Devcom Mid-America, 45 F.3d 231, 235 (7th Cir. 1995) (citing *Peak* as an authority for the proposition that loading into RAM creates a "copy"); CSU Holdings v. Xerox, 910 F. Supp. 1537, 1541 (D. Kan. 1995) ("We agree with [*Peak*] that transferring a computer program from a storage device to a computer's RAM constitutes a copy for purposes of copyright law."); Advanced Computer Servs. of Mich., Inc. v. MAI Sys. Corp., 845 F. Supp. 356, 363-64 (E.D. Va. 1994) (citing *Peak* as support for holding that RAM copies maintained for minutes infringe as copies).

25. *Peak*, 991 F.2d at 513.

26. *Id.* at 518.

27. The Ninth Circuit's opinion in *Peak* fails to explain why § 117(a), codified at that time as § 117, did not place Peak's activity outside the scope of MAI's exclusive rights. Section 117, as revised in 1980, provided that "it is not an infringement for the owner *of a copy* of a computer program to make *or authorize* the making of another copy

In the wake of *Peak,* any ISO without a license to make copies of protected software faced copyright liability for activities essential to its business. Computer hardware manufacturers sold hardware, but licensed the software that enabled it to function.[28] These licenses allowed equipment purchasers to boot up their machines (copying software into RAM in the process), but in some instances barred third parties from doing so.[29] The inability of ISOs to turn on equipment without a license from the computer equipment manufacturer gave the manufacturers a competitive advantage in the service market—at least to the extent that manufacturers controlled license terms.

The CMCAA addressed this anticompetitive use of copyright law in order to restore competition in the service market.[30] The statutory safe harbor it created, § 117(c), reads:

---

or adaptation of that computer program provided . . . that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner . . . ." 17 U.S.C. § 117(1) (Supp. IV 1980) (emphasis added). The Ninth Circuit dismissed this exclusion in a single footnote, stating that "[s]ince MAI licensed its software, the Peak customers do not qualify as 'owners' of the software and are not eligible for protection under § 117." *Peak*, 991 F.2d at 518 n.5. The Ninth Circuit did not address whether the owner of *the copy* (presumably the party that hired Peak) had authorized Peak to make a RAM copy in order to utilize the equipment. The opinion has been criticized for failing to distinguish between ownership of copyright in software and ownership of a single copy of that software. *See, e.g.*, DSC Commc'ns. Corp. v. Pulse Commc'ns, Inc., 170 F.3d 1354, 1360 (Fed. Cir. 1999) ("[A] party who purchases copies of software from the copyright owner can hold a license under a copyright while still being an 'owner' of a copy of the copyrighted software for purposes of section 117."); MELVILLE B. NIMMER & DAVID NIMMER, 2 NIMMER ON COPYRIGHT § 8.08[B][1][c] (2006) (characterizing the Ninth Circuit's logic as "inadequate"). A district court not only repeated this mistake, but went so far as to omit "of a copy" when reciting the statute. *See* Advanced Computer Servs. of Mich., Inc. v. MAI Sys. Corp. 845 F. Supp. 356, 367 (E.D. Va. 1994) ("Section 117 only permits 'the owner . . . of a computer program to make or otherwise authorize the making of another copy.'").

28. *See, e.g.*, *Peak*, 991 F.2d at 517 n.3 (quoting license term that software was equipment manufacturer's "valuable and exclusive property"); *DSC*, 81 F.3d at 599 (noting software license accompanying hardware sale); *CSU Holdings*, 910 F. Supp. at 1540-43 (noting manufacturer sold copiers while selling software licenses). Software is typically licensed rather than sold. *See* Christian Nadan, *Software Licensing In the 21st Century: Are Software "Licenses" Really Sales, and How Will the Software Industry Respond?*, 32 AIPLA Q.J. 555, 557 (2004); *see also* Andrew Rodau, *Computer Software: Does Article 2 of the Uniform Commercial Code Apply?*, 35 EMORY L.J. 853, 862 (1986).

29. *See, e.g.*, *Peak*, 991 F.2d at 517 n.3 (describing a license that had the practical effect of prohibiting third parties from activating equipment that made RAM copies when booted).

30. *See* H.R. REP. NO. 105-551, pt. 1, at 27 (1998).

> [I]t is not an infringement for the owner or lessee of a machine to make or authorize the making of a copy of a computer program if such copy is made solely by virtue of the activation of a machine that lawfully contains an authorized copy of the computer program, for purposes only of maintenance or repair of that machine, if—
>
> (1) such new copy 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 that 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.[31]

Before *StorageTek,* no federal court of appeals had construed this statutory provision.[32]

B. The DMCA's Legal Reinforcement for TPMs: 17 U.S.C. § 1201

Technical protection measures (TPMs) introduce artificial barriers restricting the access, copying, and use of digital works.[33] By raising the cost of copying digital works, TPMs alleviate the "public goods" problem created by the very low cost of copying works relative to the cost of creating original works.[34] TPMs constitute a form of "self-help" through which content owners take extra-legal measures to control their works.[35] Self-help measures may be a precondition for legal protections, may be encouraged and reinforced by legal protections, or may disqualify one from legal

---

31. 17 U.S.C. § 117(c) (2000).

32. Storage Tech. Corp. v. Custom Hardware Eng'g. & Consulting, Inc. (*StorageTek II*), 421 F.3d 1307, 1311 (Fed. Cir. 2005).

33. TPMs may prevent access or copying altogether; limit access to particular individuals, particular hardware, or particular regions; or prevent viral or multi-generational copies, for instance by disallowing further copying of copies, or by artificially introducing degradation into each copy. TPMs need not be insurmountable to be effective. A surmountable TPM may still be effective by raising the cost (including time, effort, and resources) of unauthorized access or copying.

34. This problem has been recognized for decades. *See* Kenneth J. Arrow, *Economic Welfare and the Allocation of Resources for Invention*, 9 (RAND Corporation, Research Paper No. P-1856-RC, 1959) ("In the absence of special legal protection, [one] cannot however simply sell information on the open market. Any one purchaser can destroy the monopoly, since he can reproduce the information at little or no cost."), *available at* http://www.rand.org/pubs/papers/2006/P1856.pdf (last visited Feb. 18, 2007). For a recent discussion, see Lee Kovarsky, *A Technological Theory of the Arms Race*, 81 IND. L.J. 917, 919-21 (2006).

35. Douglas Lichtman, *How the Law Responds to Self-Help*, 1 J.L. ECON. & POL'Y 215, 216 (2005).

protections.[36] TPMs may even contravene legal rights to access, copy, or use works.[37] In some circumstances, legal support for self-help, through liability or penalties for TPM circumvention, may be beneficial; anti-circumvention laws may discourage a socially wasteful "arms race" between protection and circumvention technologies.[38]

By 1998, the content industries demanded legal reinforcement of TPMs used to protect digital works.[39] The WIPO Copyright Treaty also required the U.S. to provide legal remedies to authors where TPMs were circumvented to infringe copyrights.[40] The Senate Report reflected these driving concerns behind Title I of the DMCA:

---

36. *Id.* at 257.

37. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, 135-41 (1999). Lawrence Lessig has pointed out that where a TPM prevents lawful uses of a work, such as fair use, the theoretical right to engage in fair use loses practical value unless it can be legally enforced—an example of statutory law superseded by the law of software code. Lessig argues that software code has greater potential than legal code to create regulations and limitations on what users can do, a potential that raises a host of policy questions regarding the architecture, norms, and legal frameworks governing the internet. *See id.*

38. *See* Dan L. Burk, *Muddy Rules for Cyberspace*, 21 CARDOZO L. REV. 121, 172 (1999). In the absence of legal penalties to discourage the circumvention of TPMs and the development of circumvention technologies, the use of TPMs to create restrictions on digital works might become an unchecked "arms race," with one side constantly expending resources to create new barriers while another side spends resources to overcome them. Such an arms race is inefficient because it diverts resources that could be directed towards the development or acquisition of content, just as a real arms race diverts resources away from other forms of economic development. *See id.*; *cf.* Lee Kovarsky, *A Technological Theory of the Arms Race*, 81 IND. L.J. 917, 917-19, 945 (2006) (arguing that the inefficiency of arms races is under-theorized and stems primarily from cannibalization of authors' ability to choose an optimal mix of copyright and self-help measures). In addition, Doug Lichtman points out that at least in the context of copyright and digital rights management, "there is no reason to believe th[e] back and forth [of an arms race] would yield anything close to an optimal division between rights and restrictions." Lichtman, *supra* note 35, at 240 (2005). Lichtman notes that the effectiveness of the DMCA against such an arms race has been disappointing, in part because of the difficulty in identifying, establishing jurisdiction over, and extracting judgments from those that circumvent TPMs. *Id.* at 232-33. Lichtman identifies the general problem of prohibitive expense in enforcing copyright against individuals. *Id.* at 242. Similarly, Glenn Lunney questions the practicality of § 1201(a)(1) because it requires lawsuits against individual users. Glenn Lunney, *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, VIRGINIA L. REV. (2001). *StorageTek* thus may represent a rare case where § 1201(a)(1) enforcement was practical.

39. Peter S. Menell, *Envisioning Copyright Law's Digital Future*, 46 N.Y.L. SCH. L. REV. 63, 134 (2002).

40. Article 11 of the WIPO Copyright Treaty reads:

> Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy. Legislation implementing the [World Intellectual Property Organization] treaties provides this protection and creates the legal platform for launching the global digital on-line marketplace for copyrighted works. It will facilitate making available quickly and conveniently via the Internet the movies, music, software, and literary works that are the fruit of American creative genius. It will also encourage the continued growth of the existing off-line global marketplace for copyrighted works in digital format by setting strong international copyright standards.[41]

With these concerns in mind,[42] Congress passed Title I of the DMCA.[43] The central anti-circumvention provision, § 1201(a)(1)(A), states, "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[44]

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

WIPO Copyright Treaty, art. 11, Dec. 20, 1996, S. Treaty Doc. No. 105-17, at 1 (1997), 36 I.L.M. 65, *available at* http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html.

41. S. REP. NO. 105-190, at 8 (1998).

42. *See* Menell, *supra* note 39, at 134. Nonetheless, the final DMCA text did not exclusively reflect the concerns of content owners. Negotiation and lobbying efforts resulted in some exclusions sought by technology firms. *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 522-23 (1999).

43. Title I of the DMCA was formally known as the WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998, but is commonly referred to simply as the DMCA. WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998, Pub. L. 105-304 § 101, 112 Stat. 2860, 2861 (1998).

44. Section 1201(a) of Title 17 of the United States Code reads, in relevant part:

> (1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title.
>
> (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

Two views of § 1201 have since emerged. The "paracopyright" view is that § 1201 creates independent property rights that center on the TPMs circumvented, not the works accessed or copied.[45] Under this view, if a DVD encryption scheme, such as CSS,[46] controls access to some protected works, then circumventing it to gain access to a public domain work, or to make fair use of a protected work, would result in DMCA liability.[47] Dicta by the Second Circuit in *Universal City Studios, Inc. v. Corley* suggested that the DMCA prohibits access even for fair use: "Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique or in the format of the original."[48] Similarly, in *Davidson & Associates v. Jung*, the Eighth Circuit focused on the existence of access controls rather than whether material being protected by a TPM was copyrightable.[49]

However, two subsequent appellate cases have rejected the paracopyright view. In *Chamberlain Group, Inc. v. Skylink Technologies*, the Fed-

---

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

The DMCA exhibits an asymmetry in that it does not ban circumvention of anti-copying technology while banning the trafficking in devices for that purpose.

45. H.R. REP. NO. 105-551, pt. 2, at 24 (1998). As noted in the House Report, the term "paracopyright" was used in a September 16, 1997 letter sent to Congress by concerned law professors. *Id.*

46. CSS, or Content Scramble System, is the encryption system used to encrypt commercial DVDs. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 436-37 (2d Cir. 2001).

47. See Burk, *Anticircumvention Misuse*, *supra* note 6, at 1095, for a discussion that offers this interpretation and identifies resulting problems. Other language in the DMCA fails to clarify the relation between the § 1201 and § 106 rights; for instance, § 1201(c) states that § 1201 does not "affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title," but this is itself ambiguous, compromise language with unclear impact on the ambiguous, compromise language of § 1201(a).

48. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 459 (2d Cir. 2001). The court, however, did not hold that circumvention to make fair use violated the DMCA, because the appellants had not claimed to be making fair use of copyrighted works, other methods of making fair use of the DVDs in question were possible, and the effects on possible fair use of others were not evident. *Id.*

49. Davidson & Assocs. v. Jung, 422 F.3d 630 (8th Cir. 2005). *See* A.H. Rajani, Note, Davidson & Associates v. Jung: *(Re)interpreting Access Controls*, 21 BERKELEY TECH. L.J. 365, 376 (2006).

eral Circuit held that the anti-trafficking provision of the DMCA, § 1201(a)(2), was not violated where no relationship existed between circumvention and a violation of one of the exclusive rights defined in the Copyright Act.[50] The Federal Circuit signaled that the DMCA protections were not independent property rights, but served only to protect the rights already enumerated in the Copyright Act.[51] Similarly, in *Lexmark International, Inc. v. Static Control Components, Inc.*, the Sixth Circuit drew a strong distinction between appropriation of protected expression and use of functionality, holding that that where a TPM prevented use—but not reproduction—of protected software, then a device that circumvented the TPM did not violate § 1201(a)(2) of the DMCA.[52] The court also held that the DMCA only protects access to works protected by the Copyright Act.[53] A concurring opinion went further, stating that if underlying copying were shown to be fair use, there would be no violation of the DMCA.[54]

Chamberlain and *Static Control* illustrate how the paracopyright interpretation of the DMCA could restrict activities far-removed from the distribution of digital content. While *Universal* concerned the kind of activity the DMCA was enacted to address (enabling widespread copying of digitized movies), both *Chamberlain* and *Static Control* concerned manufacturers (of garage door openers and printers, respectively) that sued to block after-market activities of potential competitors (selling remote control devices and chips for remanufactured toner cartridges).[55] These attempts to use the DMCA to control competition for after-market sales resembled earlier attempts to use ordinary copyright to control post-sale service, as seen in *Peak*.[56] By declining to adopt the paracopyright view, the *Chamberlain* and *Static Control* courts stymied these efforts.[57]

---

50. Chamberlain Group, Inc. v. Skylink Techs., 381 F.3d 1178, 1204 (Fed. Cir. 2004). Chamberlain, a manufacturer of garage door openers (GDOs) had used "rolling code" technology to restrict access to the GDO. *Id.* at 1183. Skylink, a maker of after-market GDO transmitters, had circumvented this restriction so that its universal transmitter could interoperate with GDOs sold by Chamberlain. The opinion by Judge Gajarsa, citing § 1201(c)(1), found no DMCA violation in the absence of a nexus to infringement of Chamberlain's § 106 rights. *Id.*

51. *Id.* at 1204.

52. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 546-50 (6th Cir. 2004).

53. *Id.* at 550.

54. *Id.* at 552-53 (Merritt, J., concurring) (stating that the DMCA requires plaintiff to show defendant circumvented TPM for the purpose of pirating a protected work).

55. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435-36 (2d Cir. 2001); *Chamberlain*, 381 F.3d at 1183-85; *Static Control*, 387 F.3d at 530-31.

56. *See Chamberlain*, 381 F.3d at 1183; *Static Control*, 387 F.3d at 530; MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 513-16 (9th Cir. 1993) (discussing injunctions

Such was the state of the law prior to *StorageTek*.

II. *STORAGETEK*: FACTS AND CASE HISTORY

This Part discusses the facts of *StorageTek* and the proceedings at the district court. Section II.A presents an overview of the technology at issue—a tape library system manufactured by plaintiff Storage Technology Corp. ("StorageTek"), the software that was licensed, and the conduct at issue—the RAM-copying of software and TPM circumvention by defendant ISO Custom Hardware Engineering ("CHE"). Section II.B recounts the procedural history of *StorageTek*.

A. Factual Record: The Computer System and the ISO's Conduct

CHE was hired to maintain a StorageTek tape library system, which comprised multiple tape library units coordinated by a single Library Management Unit (LMU)—a computer with a processor, RAM, and a hard disk containing specialized software.[58] Each tape library included a Library Control Unit (LCU)—another computer with a processor and RAM—that controlled and monitored a huge Library Storage Module (or "Silo") containing racks of tapes, tape drives, and a robotic arm.[59] Each tape library operated like a data jukebox, storing and retrieving massive amounts of data distributed across thousands of tapes, which the robotic arm inserted into the tape drives as needed.[60]

When something went wrong with the operation of the robotic arm, numeric fault system codes were generated by software running in the

---

sought by MAI). *Davidson* blocked the use of third-party servers for a multiplayer video game—arguably an after-market competition issue as well. However, the court's comment that "games can be easily copied and distributed over the Internet" suggests that the court viewed the case through the lens of core DMCA concerns about distribution of digital content. *See Davidson*, 422 F.3d at 633, 637.

57. Indeed, the entire panel in *Static Control* agreed that "the [DMCA] was not intended by Congress to be used to create a monopoly in the secondary markets for parts or components of products that consumers have already purchased." *Id.* at 553 (Feikens, J., concurring in part).

58. The following descriptions and diagrams are based on: the district court's findings of facts, Storage Tech. Corp. v. Custom Hardware Eng'g (*StorageTek I*), No. 02-12102, 2004 WL 1497688, at *1-2 (D. Mass. July 2, 2004); the description provided in the Federal Circuit's initial opinion, *StorageTek II*, 421 F.3d at 1309-10; and StorageTek's specifications for the 9310 tape library [hereinafter *9310 Specifications*], *available at* http://www.storagetek.com/products/product_page32.html (last visited Jan. 25, 2007).

59. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *1; *StorageTek II*, 421 F.3d at 1309-10; *see also 9310 Specifications*, *supra* note 58.

60. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *1; *9310 Specifications*, *supra* note 58.

LCU.[61] The LCU could be set to various maintenance levels—basically logging levels—ranging from zero to nine.[62] Above level zero, the generated fault codes were packaged into an "Event Message" sent over the network to the LMU, which stored the messages in an error log on its hard drive.[63]

A system called GetKey allowed technicians to set the maintenance level by entering a password on the LMU, keyed to the LMU's serial number and desired level.[64] StorageTek technicians could obtain these passwords by telephone,[65] but CHE resorted to a device, called the Library Event Manager (LEM), that tried successive passwords until it found one that set the desired level.[66] After the GetKey password was accepted, the system was then rebooted (which propagated the change to the LCU).[67] Later, CHE discovered it could simply send a file to the LCU as it rebooted, which mimicked a file normally sent by the LMU.[68] This method eliminated the need to use GetKey, and starting in March 2003, CHE phased out the LEM in favor of a new device, the Enhanced LEM (ELEM), which employed the newer method.[69]

A system reboot was required to make the new level take effect.[70] Rebooting caused the LMU first to copy its own software from disk into

---

61. *StorageTek II*, 421 F.3d 1307, 1310 (Fed. Cir. 2005).

62. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *2.

63. *StorageTek II*, 421 F.3d at 1310. The district court characterized the Maintenance Code differently than did the Federal Circuit, finding that "[w]hen activated . . . [it] runs a series of diagnostic tests, provides information as to the nature of the problem and where the system difficulties have occurred or are likely to blossom, and performs other maintenance-specific operations." *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *2. Yet, the district court goes on to note that "event logging" is among the most important of the diagnostic functions performed by the code, and nothing in either the district court or Federal Circuit's opinion indicates that CHE was making use of any features other than event logging. *See id.*

64. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *2; *StorageTek II*, 421 F.3d at 1310. Although this Note follows the Federal Circuit in using the term "password," the password was not an arbitrary set of characters like a user-created password for a computer, but an algorithmically generated string based on the serial number of the hardware and a specified maintenance level, perhaps more aptly compared to a CD-ROM registration key. *See id.*

65. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *2.

66. *Id.* at *3; *StorageTek II*, 421 F.3d at 1310.

67. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *2; *StorageTek II*, 421 F.3d at 1310.

68. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3; *StorageTek II*, 421 F.3d at 1310.

69. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3.

70. *StorageTek II*, 421 F.3d at 1310.

RAM, then to send a copy of the LCU software across the network into the LCU's RAM.[71] The factual record reveals nothing that could stop these software copies from being created upon rebooting.[72] During the term of CHE's maintenance contract, the LEM (or ELEM) would reside on the network between the LCU and LMU, intercepting Event Messages sent by the LCU and forwarding them to CHE headquarters in Arizona, where technicians would interpret them to diagnose problems.[73] At the end of the three-year contract, the system was again rebooted.[74]

StorageTek sold customers the tape library hardware, but merely licensed the software.[75] Two disputed features of the license played a role in the case. First, StorageTek contended that the licenses excluded "maintenance code" that "detects, records, displays and/or analyzes malfunctions in [the] Equipment."[76] Second, it claimed that non-transferability provisions precluded the license from covering ISOs hired by the purchaser.[77]

Diagram 1 illustrates how StorageTek technicians used GetKey to set the maintenance level. Diagram 2 depicts use of the LEM to circumvent GetKey. Diagram 3 shows how CHE's ELEM set the maintenance level by interacting only with the LCU, not the LMU or GetKey.

---

71. *Id.* at 1309.

72. *Id.* As CHE's appellate brief noted, "[t]he only way to prevent the 'Maintenance Code' from being loaded or executed on activation is to leave the [tape library] System turned off." Non-Confidential Brief of Defendants-Appellants Custom Hardware Engineering & Consulting, Inc. and David York at 12, Storage Tech. Corp. v. Custom Hardware Eng'g, Inc., 421 F.3d 1307 (Fed. Cir. 2005) (No. 04-1462), 2004 WL 5003204.

73. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3; *StorageTek II*, 421 F.3d at 1310.

74. *StorageTek II*, 421 F.3d at 1312.

75. *Id.* at 1310.

76. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *2 ("Plaintiff licenses the use of the Functional Code when it sells its systems. However, it retains exclusive use of the Maintenance Code portion and zealously guards it by means of its copyright registrations and by disabling and enabling the functions of the code with its GetKey.").

77. Corrected Non-Confidential Brief of Plaintiff-Appellee Storage Technology Corporation at 23-24, Storage Tech. Corp. v. Custom Hardware Eng'g, Inc., 421 F.3d 1307 (Fed. Cir. 2005) (No. 04-1462), 2004 WL 5003205.

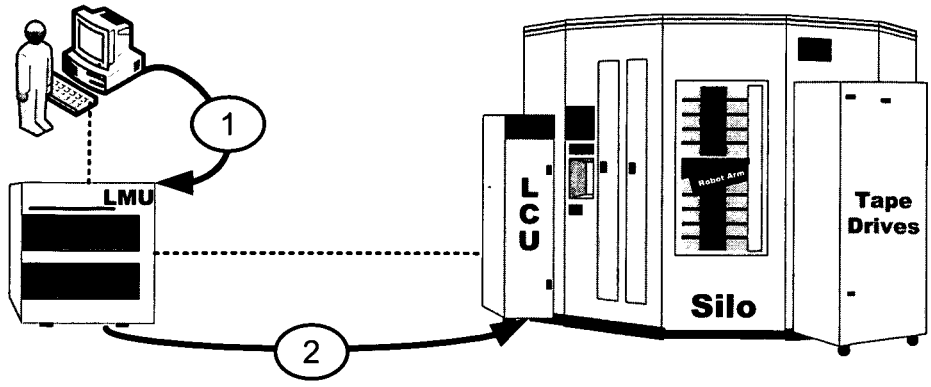

Diagram 1: Maintenance provided by StorageTek: (1) StorageTek technician enters password into workstation connected to the LMU. (2) In the LMU, GetKey software accepts password, causing LMU to send a file to the LCU (attached to the Silo). (3) The LCU begins sending Event Messages, to the LMU, which stores them in a log file readable by the technician.

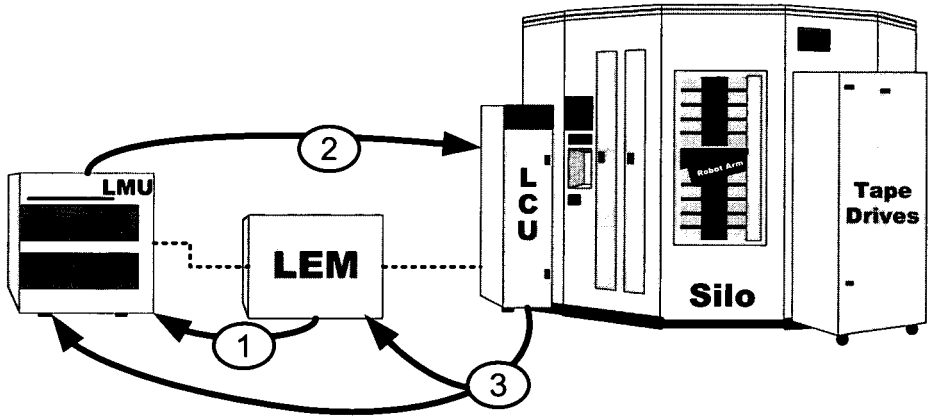

Diagram 2: LEM Method: (1) The LEM tries many passwords, each sent to the LMU. (2) In the LMU, GetKey software accepts correct password and the LMU sends a file to LCU (3) Upon rebooting, the LCU begins sending Event Messages to the LMU, which are copied by the LEM and sent to CHE over the internet (not depicted).

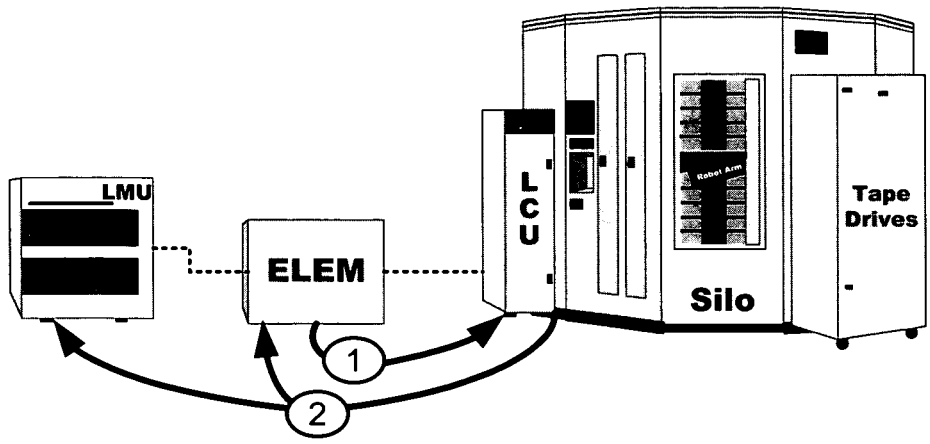

Diagram 3: ELEM Method: (1) The ELEM, instead of interacting with GetKey, sends a file (normally sent by the LMU) to the LCU (2) Upon rebooting, the LCU begins sending Event Messages to the LMU, which are copied by the ELEM and sent to CHE.

B. Procedural History

In October 2002, StorageTek sued CHE in the District of Massachusetts.[78] StorageTek alleged: (i) violation of its § 106 reproduction right through CHE's copying of StorageTek's "maintenance code" and (ii) through CHE's copying of Event Messages using the LEM/ELEM, (iii) violations of DMCA § 1201(a)(1) based on CHE's circumvention of GetKey, (iv) misappropriation of trade secrets, based on the theory that intercepted Event Messages were trade secrets, and (v) patent infringement.[79]

The district court granted StorageTek's motion for a preliminary injunction.[80] The district court held that StorageTek was likely to succeed in showing copyright infringement of the maintenance code,[81] on its DMCA claims,[82] and on the trade secret claims.[83] Regarding the copyright infringement claim, the district court rejected CHE's § 117(c) defense as

78. Complaint for Damages and Injunctive Relief at 1, Storage Tech. Corp. v. Custom Hardware Eng'g, Inc., No. 02-12102, 2002 WL 33928462, (D. Mass. Oct. 28, 2002).

79. Third Amended Complaint for Damages and Injunctive Relief at 2-3, Storage Tech. Corp. v. Custom Hardware Eng'g, Inc., No. 02-12102-RWZ, 2004 WL 4908848, (D. Mass. Mar. 31, 2004); *see* Storage Tech. Corp. v. Custom Hardware Eng'g, Ltd., No. 02-12102-RWZ, 2006 WL 1766434, at *1 (D. Mass. June 28, 2006).

80. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *5.

81. *Id.* at *3.

82. *Id.* at *4.

83. *Id.* at *4-5.

well as its defense that the RAM copies it made were permitted under the license granted by StorageTek to the machine owner.[84] The district court did not reach StorageTek's claim that copying the Event Messages constituted additional infringement.[85] The district court enjoined CHE from circumventing the password, intercepting and displaying the error messages, or causing the copying of the maintenance code.[86]

CHE appealed.[87] Because StorageTek's complaint had included a patent claim (adjudicated prior to the appeal) CHE's appeal landed before the Federal Circuit.[88] The Federal Circuit vacated the preliminary injunction in a split-panel decision, concluding that StorageTek was unlikely to prevail on *any* of the key issues.[89] StorageTek then petitioned for rehearing, which was denied by the same panel, which issued a supplemental opinion clarifying aspects of its original decision.[90]

III. ANALYSIS OF *STORAGETEK*

This Part analyzes the key holdings of the Federal Circuit concerning the § 117(c) safe harbor, StorageTek's anti-circumvention claims, and the software license terms. Section III.A considers the court's broad construction of the safe harbor, focusing on the court's interpretation of "maintenance," its analysis of CHE's purpose, and the test by which the court found certain software code necessary for activation. Section III.B assesses the court's extension of its *Chamberlain* DMCA analysis to *StorageTek*. Section III.C explores the court's finding of an implied license and its distinction between contract law and copyright law claims.[91]

---

84. *Id.* at *4.

85. *Id.* at *3 n.3.

86. *Id.* at *6.

87. *StorageTek II*, 421 F.3d at 1307.

88. *Id.* at 1310. Federal Circuit jurisdiction depends on the claims in the complaint, not on the subject of the appeal. 28 U.S.C. § 1295(a)(1) (2000).

89. *StorageTek II*, 421 F.3d at 1321.

90. Storage Tech. Corp. v. Custom Hardware Eng'g, Inc. (*StorageTek III*), 431 F.3d 1374 (Fed. Cir. 2005).

91. The Federal Circuit also rejected the trade secret claims. *StorageTek II*, 421 F.3d at 1321. The court ruled that StorageTek's error codes were not trade secrets because the information was "not actually secret," citing "overwhelming evidence" that from 1987 to 1992 StorageTek had made the information freely available, including displaying the messages on display panels to users. The court deemed StorageTek's subsequent efforts to keep the codes secret irrelevant. The court also dismissed StorageTek's argument that while the error messages were in the public domain, particular event error messages sent corresponding to the malfunction of a specific machine remained trade secrets. This argument, the court ruled, amounted to a claim that although the customer owns the ma-

A. The § 117(c) Maintenance Safe Harbor Analysis

The district court ruled that CHE did not qualify for the § 117(c) safe harbor on three grounds.[92] First, CHE activated the machines not "for purposes only of maintenance or repair," as required by § 117(c) itself,[93] but to circumvent GetKey, set the maintenance level, and intercept the Event Messages.[94] Second, CHE did not destroy the RAM copies immediately, as required by § 117(c)(1), because it left the copies in RAM for the duration of the maintenance contract.[95] Third, the district judge implied that code unnecessary for activation was accessed or used, in violation of § 117(c)(2).[96]

Thus, whether CHE's activities were within the safe harbor turned on three issues: (1) whether CHE activated the tape libraries "for purposes only of maintenance or repair,"[97] (2) whether it destroyed the ensuing RAM copies "immediately" after the maintenance was completed,[98] and (3) whether the code used was "necessary for that machine to be activated."[99] The Federal Circuit, taking a quite different view of the same facts, answered each of these questions affirmatively. This Section examines the Federal Circuit's analysis of each of these issues, in turn.[100]

1. *Purpose: What is Activation "for Purposes Only of Maintenance or Repair"?*

To fall within the safe harbor, the activation that caused the copying had to be "for purposes *only* of maintenance or repair."[101] The district court had agreed with StorageTek that CHE was outside the safe harbor

---

chine, the factual reason that a customer's particular machine is malfunctioning is owned by StorageTek—a claim the court found implausible on its face. *StorageTek II*, 421 F.3d at 1319-21. Because the trade secret holding did not substantially change existing law, this Note focuses on the copyright and DMCA issues raised in the case.

92. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3.

93. 17 U.S.C. § 117(c) (2000).

94. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3.

95. *Id.*

96. *Id.*

97. *See* 17 U.S.C. § 117(c).

98. *See id.* § 117(c)(1).

99. *See id.* § 117(c)(2).

100. Other elements set forth in the main clause of § 117 were not in dispute. The owner of the machine had authorized the copy by hiring CHE to maintain the equipment. Rebooting the machine automatically caused the software to be copied into RAM. Because the program was actually stored on the LMU and loaded over the network, the LCU arguably did not "lawfully contain[] an authorized copy of the computer program," but the courts did not address this technical, formalistic point.

101. 17 U.S.C. § 117(c) (emphasis added).

because its purposes included circumventing GetKey, changing the maintenance level, and reading Event Messages.[102] The district judge also expressed concerns about CHE's business practices in servicing StorageTek equipment, commenting, "To do [CHE's] work effectively and efficiently, [CHE], too, needed a diagnostic tool, and they chose to piggyback on [StorageTek's] Maintenance Code."[103]

The Federal Circuit arrived at a different conclusion by distinguishing the *purpose* in activating the equipment from (i) the incidental steps taken, (ii) the propriety of the means employed, and (iii) possible anticompetitive motives in selecting which means to employ.[104] The Federal Circuit found that circumventing GetKey, setting the maintenance level, and reading the Event Messages were merely intermediate steps taken for the purpose of maintenance—not purposes that would disqualify CHE from the safe harbor.[105] Even CHE's alleged piggybacking, the court reasoned, concerned the propriety of the means employed, not the nature of the end pursued:

> If CHE had rebooted the storage library and loaded its own proprietary code to detect and diagnose errors in the silo, that activity would surely be considered "repair and maintenance." Merely because CHE uses StorageTek's proprietary code to do the same thing does not cause CHE's activities to no longer be "for the purpose only of maintenance or repair of that machine."[106]

Several considerations favor the Federal Circuit's analysis over that of the district court. First, as the Federal Circuit suggests, the district court approach would eliminate the safe harbor. Under the district court's broad reading of "purpose," any activity complex enough to involve subsidiary steps would involve multiple "purposes." In this instance, CHE used the LEM to circumvent GetKey, which in turn allowed reconfiguration, which in turn allowed reading Event Messages, which allowed effective monitoring. If these subsidiary "purposes" count as disqualifying under the statute, then only the simplest, single-step activities could ever be "only for purposes of maintenance or repair." Since this would effectively eliminate the safe harbor, it is the wrong approach.

---

102. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3; Non-Confidential Brief of Plaintiff-Appellee Storage Technology Corporation at 19, Storage Tech. Corp. v. Custom Hardware Eng'g, Inc., 421 F.3d 1307 (Fed. Cir. 2005) (No. 04-1462), 2004 WL 5003205.

103. *Id.*

104. *StorageTek II*, 421 F.3d at 1315.

105. *Id.*

106. *Id.*

Second, simply tallying up all these "purposes" ignores the hierarchy involved—the difference between an end that remains constant and the changing means to achieve it.[107] Yet the facts of *StorageTek* illustrate this distinction. When the ELEM technique was developed, the LEM was discarded.[108] Where CHE found machines already configured, neither method was necessary.[109] The flexibility in the means employed contrasts with, and indeed resulted from, the constancy of the ISO's maintenance purpose.

Third, if every node in the hierarchy of means and ends is a "purpose" under § 117, then so should CHE's over-arching purpose of making a profit. ISOs do not perform maintenance as an end in itself; CHE performed maintenance for the "purpose" of making money. Yet disqualifying an ISO based on this "purpose" would be absurd, since competing in the service market to make a profit is the very activity the statute was created to protect.

Finally, under the Federal Circuit's approach, the language of § 117(c)(1) remains a meaningful limitation on ISO activity. The Federal Circuit correctly focused not on "counting up" multiple purposes, but on whether CHE's activities fit within the purpose of maintenance.[110] This treatment suggests that the limiting factor is consistency. The presence of an extra purpose *inconsistent* with maintenance, presumably, would still close the safe harbor.

By holding that a maintenance purpose pursued by anticompetitive means nonetheless qualifies for the safe harbor, the court deftly separated the copyright issue, whether CHE's purpose disqualified it from the safe harbor, from a claim that CHE engaged in anticompetitive "piggybacking" to achieve that purpose, which would be better addressed under unfair competition laws. This exhibits a recurrent theme of the court's decision: refusal to create copyright liability or grant copyright remedies for acts that, while perhaps unlawful, do not constitute the unauthorized copying

---

107. *See StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3 ("[CHE] use[s] their LEM or ELEM mechanisms for the express purpose of circumventing plaintiff's GetKey and resetting the Maintenance Level. . . . Defendants copy the Code . . . not just for repair, but also for the express purpose of circumventing plaintiff's security measures, modifying the Maintenance Level, and intercepting plaintiff's Event Messages.").

108. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3.

109. CHE's appellate papers indicate that about one-third of the machines serviced already had maintenance levels set above zero. Non-Confidential Reply Brief of Defendant-Appellants Custom Hardware Engineering & Consulting, Inc. and David York at 22, Storage Tech. Corp. v. Custom Hardware Eng'g, Inc., 421 F.3d 1307 (Fed. Cir. 2005) (No. 04-1462), 2004 WL 5003204.

110. *See StorageTek II*, 421 F.3d at 1315.

of protected expression or otherwise infringe the exclusive rights enumerated under section 106 of the Copyright Act.

2. Duration: What is the Duration of Maintenance?

Section 117(c)(1) requires that the RAM copies be "destroyed immediately after the maintenance or repair is completed."[111] Although the statute defines "repair" and "maintenance," the definitions do not resolve the scope of each term.[112] The key issue was how long "maintenance" may last. The district court adopted StorageTek's position that because CHE left the copies in RAM for the three-year duration of the maintenance contract, CHE had failed to destroy the copies "immediately."[113] Vacating the lower court's ruling, the Federal Circuit held that because CHE rebooted the machines at the end of the three-year monitoring period, the copy was "destroyed immediately after the maintenance."[114]

The Federal Circuit based its holding on (a) the statutory language, (b) the legislative history, and (c) the policy goal of § 117(c). First, the Federal Circuit reasoned that Congress intended to identify distinct activities by using the different terms "repair" and "maintenance," and that "'maintenance' has a much broader temporal connotation."[115] Second, the court stated that inclusion of "checking the proper functioning of [] components" in the legislative history indicated that Congress intended the term to cover "monitoring systems for problems."[116] Third, the court stated that such an interpretation promoted Congress' stated policy goal of avoiding "artificial restraints on companies engaged in legitimate repair and maintenance activities."[117]

This reading of "maintenance" was not inevitable. Another plausible view, suggested by Judge Rader's dissent, is that maintenance is distinguished from repair because it involves preventative (but still temporally

---

111. 17 U.S.C. § 117(c)(1) (2000).

112. Section 117(d) provides definitions for "repair" and "maintenance":

> (1) the "maintenance" of a machine is the servicing of the machine in order to make it work in accordance with its original specifications and any changes to those specifications authorized for that machine; and
>
> (2) the "repair" of a machine is the restoring of the machine to the state of working in accordance with its original specifications and any changes to those specifications authorized for that machine.

17 U.S.C. § 117(d) (2000).

113. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3.

114. *StorageTek II*, 421 F.3d at 1312-13.

115. *See id.* at 1312.

116. *Id.* at 1312.

117. *Id.*

discrete) tasks.[118] This view is also consistent with the statutory definitions. Moreover, it fits with the legislative history because most of the examples of maintenance therein are temporally limited, and "checking the proper functioning of equipment" could easily describe a one-hour activity rather than a three-year monitoring project.[119] Finally, since the CMCAA was a response to cases like *Peak*, Congress arguably had in mind a temporally limited conception of service, as was involved in that case, when it enacted § 117(c).[120]

The Federal Circuit's analysis, however, has the advantage that it allows for efficient computer maintenance techniques that involve ongoing continuous monitoring during everyday operations, rather than discrete periods of scheduled downtime.[121] Though Congress was responding to *Peak*, it was also mindful of ongoing technological advances,[122] and presumably intended the statutory safe harbor to continue to preserve competition as service techniques evolve along with technology.[123] Thus, even if

---

118. *Id.* at 1322.

119. *See* H.R. REP. NO. 105-551, pt. 1, at 28 (1998) ("These acts can include, but are not limited to, cleaning the machine, tightening connections, installing new components such as memory chips, circuit boards and hard disks, checking the proper functioning of these components, and other similar acts."). Note that the word "acts" arguably also supports the view of maintenance as temporally discrete.

120. *Peak* involved repairs to malfunctioning circuit boards, as opposed to the years-long monitoring at issue in *StorageTek*. MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 513 (9th Cir. 1993).

121. Minimizing downtime is increasingly important as companies seek "high availability" systems and vendors tout features that reduce downtime. *See, e.g.*, Doug Dineley, *Improve Availability of Enterprise Data; For Those Striving to Avoid System Downtime, Change is Enemy No. 1*, INFOWORLD, Mar. 12, 2007 (emphasizing importance of high availability systems); High Availability, http://www.linuxvirtualserver.org/HighAvailability.html (last visited Mar. 16, 2007) (touting advantages of a system that allows upgrades without bringing down the system).

122. Starting with the title, "Digital Millennium Copyright Act," the legislative history of the DMCA evinces an awareness of rapid changes in both technology and commerce, as well as a concern not to stand in the way of such advances: "Much like the agricultural and industrial revolutions that preceded it, the digital revolution has unleashed a wave of economic prosperity and job growth. Today, the information technology industry is developing versatile and robust products to enhance the lives of individuals throughout the world," H.R. REP. NO. 105-551, pt. 2, at 21 (1998). The Senate Report anticipated that "rapid and dynamic development of better technologies," concerning technological protection measures. S. REP. NO. 105-190, at 15 (1998). The House Report noted that "[a]s technology advances, so must our laws." H.R. REP. NO. 105-551, pt. 2, at 25 (1998).

123. The Senate Report expressly stated that "maintenance" is "not limited to" the activities cited as examples of maintenance. S. REP. NO. 105-190, at 58 (1998). Given this open-ended language and the general awareness of dynamically evolving technolo-

the Federal Circuit stretched the statutory language to cover current maintenance practices, it may be justified in light of the purpose and the difficulty in regulating evolving technology.

By holding that Congress intended "maintenance" to encompass years-long monitoring of systems, the Federal Circuit created a wide safe harbor, but at the cost of weakening the requirement that the RAM copies be destroyed immediately after the maintenance or repair. Yet, given that the purpose of the destruction provision is, as both majority and dissent agree, "to prevent persons from invoking the protection of § 117 and then later using the copied material for a prohibited purpose," this cost is not too great.[124] For whether the code remains in the RAM of a single machine for a day or a year does not determine whether it is used for prohibited purposes. Rather, the primary danger is that the software "escapes into the wild" through the creation and distribution of additional copies (say, by posting the software on the internet). This could occur in mere seconds, regardless of whether the legitimate copy persists in RAM for an extended period.

3. *Necessity: When is Software Code Necessary for a Machine to be Activated?*

Section 117(c)(2) excludes from the safe harbor the access or use of programs (and parts of programs) that are not "necessary for that machine to be activated."[125] The district judge implied that the "maintenance code" that CHE accessed and used was not necessary for activation, such that CHE violated § 117(c)(2), but offered no analysis concerning necessity.[126]

In determining what the statute meant by "necessary" here, the Federal Circuit considered the legislative history of the CMCAA.[127] The House Report contemplated that a hardware manufacturer might provide diagnos-

---

gies exhibited throughout the bill, it is reasonable to conclude the Congress intended to authorize current and future maintenance techniques.

124. *StorageTek II*, 421 F.3d at 1322.

125. 17 U.S.C. § 117(c)(2) reads: "[W]ith respect to any computer program *or part* thereof that is *not necessary for that 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." 17 U.S.C. § 117(c)(2) (2000) (emphasis added).

126. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3.

127. *StorageTek II*, 421 F.3d at 1314. StorageTek cited this history in its brief. Corrected Non-Confidential Brief of Plaintiff-Appellee Storage Technology Corporation at 17-18, Storage Tech. Corp. v. Custom Hardware Eng'g, Inc., 421 F.3d 1307 (Fed. Cir. 2005) (No. 04-1462), 2004 WL 5003205. In denying rehearing, the Federal Circuit again addressed the legislative history in clarifying its finding that the maintenance code was necessary in this case. Storage Tech. Corp. v. Custom Hardware Eng'g, Inc. (*StorageTek III*), 431 F.3d 1374, 1376 (Fed. Cir. 2005).

tic programs that "may be loaded into RAM when the computer is turned on, but . . . did not need to be so loaded . . . for the machine to be turned on," and stated that under section 117(c)(2), "if such a program is accessed or used without the authorization of the copyright owner, the initial reproduction of the program [into RAM] shall not be deemed exempt from infringement."[128]

The Federal Circuit held that the "maintenance code" *was* necessary for activation because it was "so entangled with the functional code that the entire code *must be loaded into RAM* for the machine to function at all."[129] As the court noted in denying StorageTek's petition for rehearing, this finding of entanglement was tied to the particular facts of this case,[130] and while the court engaged in a long discussion of necessity, it did not

---

128. The House Report contains the following paragraph on § 117(c)(2):

> Third, as is made clear in paragraph (c)(2), the amendment is not intended to diminish the rights of copyright owners of those computer programs, or parts thereof, that also may be loaded into RAM when the computer is turned on, *but which did not need to be so loaded in order for the machine to be turned on*. A hardware manufacturer or software developer might, for example, provide diagnostic and utility programs that load into RAM along with or as part of the operating system, even though they market those programs as separate products—either as freestanding programs, or pursuant to separate licensing agreements. Indeed, a password or other technical access device is sometimes required for the owner of the machine to be able to gain access to such programs. In other cases, it is not the hardware or software developer that has arranged for certain programs automatically to be reproduced when the machine is turned on; rather, the owner of the machine may have configured its computer to load certain applications programs into RAM as part of the boot-up process (such as a word processing program on a personal computer). This amendment is not intended to derogate from the rights of the copyright owners of such programs. In order to avoid inadvertent copyright infringement, these programs need to be covered by subsection (c), but only to the extent that they are automatically reproduced when the machine is turned on. This legislation is not intended to legitimize unauthorized access to and use of such programs just because they happen to be resident in the machine itself and are reproduced with or as part of the operating system when the machine is turned on. According to paragraph (c)(2), if such a program is accessed or used without the authorization of the copyright owner, the initial reproduction of the program shall not be deemed exempt from infringement under subsection (c).

H.R. REP. NO. 105-551, pt. 1, at 28 (1998) (emphasis added). Senate Report 105-190 contains almost identical language. S. REP. NO. 105-190, at 57 (1998).

129. *StorageTek II*, 421 F.3d at 1314 (emphasis added).

130. *StorageTek III*, 431 F.3d at 1376.

articulate a single, bright-line test for necessity.[131] Thus, it might seem that the holding provides little guidance for future cases.

Yet the holding, when considered along with the extensive dicta, suggests a coherent approach to whether object code—that is, compiled software—is necessary for activation.[132] As a whole, the case suggests a disjunctive test under which code may qualify based on either of two distinct notions of necessity, which this Note will call *functional* necessity and *practical* necessity. Code is *functionally necessary* (i.e., necessary to *run*) if executing the instructions in the code is necessary to activate the machine and perform the essential functions for which the machine was purchased.[133] Code is *practically necessary* (i.e., necessary to *load*) if the machine's user has no practical way to keep it from loading into RAM upon activation given the factory configuration of the machine—even if the manufacturer could have designed the machine to function without loading such code.[134]

Several of the court's statements indicate that functional necessity, if established, would be sufficient to show code was necessary under § 117(c). Drawing on the definitions of "repair" and "maintenance" in § 117(d), the court stated, "the service provider must be able to cause the machine to boot up in order to determine if it '*works* in accordance with its original specifications.'"[135] The court also stated that what is "necessary" is more than "the minimal amount of code that, when loaded into RAM, *causes the machine to produce any response.*"[136] It is the execution of

131. *See StorageTek II*, 421 F.3d at 1314-15.

132. References to "code" in this section refer to compiled software, rather than source code.

133. For example, on a laptop computer, functionally necessary code would include the operating system kernel, keyboard and display drivers, and the internal system clock. Only if such software not only loads but *runs* can the laptop perform the essential functions for which it is purchased.

134. These two forms of necessity are logically independent. Code that is practically necessary to load might lack any critical function. Examples include drivers for uninstalled peripherals, code that displays logos or plays music during startup. Easter eggs—code hidden in programs by programmers that displays frivolous content in response to particular "secret" input—also fall into this class. Such code is not functionally necessary, but would be practically necessary unless the owner can configure the machine not to load the code. On the other hand, code may be functionally, but not practically, necessary in cases where the owner of a machine can configure it into a less functional or nonfunctional state. For example, it is possible, on some computers, for users to configure the machine to fail to load the operating system kernel, or to fail to load critical device drivers necessary to perform basic operations.

135. *StorageTek II*, 421 F.3d at 1314.

136. *Id.* at 1313 (emphasis added).

code—its *functioning*, not its mere loading into RAM, that causes a machine to work and respond to requests. Judge Rader, in his dissent, appeared to endorse an exclusively functional criterion of necessity, stating that "[e]ven though Storage Tek has chosen to load the maintenance code *upon* activation, the maintenance code is incidental, not indispensable, to activation."[137]

Other key statements by the court concern practical necessity, i.e., whether the owner, as opposed to the manufacturer, controls which programs load into RAM. The court noted that the legislative history stated that "software is necessary for the machine to be activated if it 'need[s] to be so *loaded* in order for the machine to be turned on.'"[138] The court rejected the simple rule that all code loaded at startup is necessary (which it noted, correctly, would read the § 117(c)(2) limitation right out of the statute).[139] The panel characterized software that machine owners independently configured to load at startup as unnecessary for activation,[140] and the language of the opinion suggests an operative distinction between "separate, 'freestanding programs,'" that the machine's owner can opt not to load, and "entangled" software that must be loaded.

Indeed, the holding rested on practical necessity; the "maintenance code" was practically necessary for activation because it was intertwined with other, functionally necessary code. This was clarified in the denial of rehearing, in which the court indicated that StorageTek's argument that its maintenance code was not functionally necessary was irrelevant given the practical necessity of loading the code:

> StorageTek argues . . . that loading the maintenance code was not "necessary" . . . because it could be loaded into RAM with one of its functions disabled. While that may be true, it does not change the fact that a copy of the entire maintenance code *must be loaded into RAM* when the machine is turned on . . . .[141]

Taken as a whole, the discussion in *StorageTek* suggests that code may be "necessary for activation" if it is *either* functionally or practically necessary. That is, it allows the practical necessity of *loading* code (rather than

137. *Id.* at 1321 (Rader, J., dissenting) (emphasis in original).

138. *Id.* at 1314 (emphasis added) (quoting H.R. REP. NO. 105–551, pt. 1, at 28 (1998)).

139. *Id.* at 1313.

140. *Id.*

141. Storage Tech. Corp. v. Custom Hardware Eng'g, Inc. (*StorageTek III*), 431 F.3d 1374, 1376 (Fed. Cir. 2005) (emphasis added).

just the necessity of *running* it) to establish that code as necessary for activation.

Four considerations suggest that this approach is a sound one. First, this approach is consistent with the legislative history. Second, it avoids placing an unreasonable burden on ISOs. Third, it creates positive incentives for manufacturers. Fourth, it is more judicially administrable than an approach that always requires *functional* necessity.

First, the legislative history's examples of unnecessary software include (i) separately marketed programs that load into RAM at startup, (ii) software the owner has configured to load at startup, and more generally, (iii) software that "may be loaded into RAM when the computer is turned on, but which did not need to be so loaded in order for the machine to be turned on."[142] These references suggest that machine owners exercise some control over the loading of any software that is *not* necessary for activation.

Second, a pure functional necessity rule would place the burden on ISO technicians to avoid either copying *or executing* code that is not functionally necessary, since under § 117(c)(2) unnecessary portions of code may not be "accessed or used other than to make such new copy by virtue of the activation of the machine."[143] Yet ISOs, like the machine owners that hire them, have little information about what non-essential parts of a program might execute in response to particular actions; thus, such a rule would in effect create potential traps for ISOs. In contrast, a practical necessity rule avoids such pitfalls by allowing a technician to use any software that cannot be configured not to load into RAM—though with the restriction that use be "only for purposes of maintenance or repair."[144]

Third, to the extent that this allows the technician to "get away with" using code that is *not* functionally necessary, it simply creates an incentive for the manufacturer—who has much better information about the internal code structure—to redesign/configure the machine so that the purchaser may easily activate the machine without loading the code into RAM. In cases where the manufacturer chooses to configure products so that only functionally necessary code is loaded at startup, then outcomes under this approach will be the same as under a functional rule—but with much less costly analysis (see the next point). This creates a positive incentive for manufacturers to make code practically necessary only if it is also functionally necessary, avoiding unnecessary "entanglement" of code.

142. S. REP. NO. 105-190, at 57 (1998).
143. 17 U.S.C. § 117(c)(2) (2000).
144. *See id.* § 117(c).

Fourth and finally, under a purely functional approach, courts would need to make determinations about what functions are essential for the machine to work within its specifications. As the Federal Circuit's discussion of functional necessity indicates, such determinations may be fact-intensive and difficult.[145] It should be easier for the court to determine whether users can control whether code loads at startup. To do so, courts can look to configuration procedures set forth in documents, such as user's guides and owner's manuals—evidence that can be easily produced. Thus, this approach is more judicially administrable than a strict functional necessity rule.

In conclusion, the court's discussion implies that *either* practical or functional necessity may establish code as necessary for activation. While this approach is justified for the reasons stated above, a more precise formulation of the test awaits future litigation.

B. The DMCA § 1201(a)(1)(A) Circumvention Claim

This Section examines the Federal Circuit's rejection of StorageTek's DMCA claims, focusing on its application of its own precedent in *Chamberlain Group, Inc. v. Skylink Technologies*, and whether this approach might spark a TPM "arms race." The court's extension of *Chamberlain* to this anti-circumvention case reflected its concern—also apparent vis-à-vis the licensing dispute—that copyright-like protections not be divorced from violations of the traditional exclusive rights granted by copyright law. While the court's approach removes DMCA liability where TPMs are used to bar activity that facilitates no infringement, this is unlikely to trigger a TPM arms race.

1. *Straightforward, but Significant: The Federal Circuit's Extension of* Chamberlain

Section 1201(a)(1)(A) of the DMCA prohibits any person from "circumvent[ing] a technological measure that effectively controls access to a work protected under this title."[146] The text suggests that a successful § 1201(a)(1)(A) claim requires showing at least five elements: (1) circumvention, (2) of a TPM, that (3) effectively (4) controls access to an identifiable work (5) that is protected by copyright.[147] Adapting the elements

145. *See StorageTek II*, 421 F.3d at 1314 ("[I]t may be difficult to determine whether particular software is necessary to make the computer function and to ascertain whether the computer is working properly."); *see also StorageTek III*, 431 F.3d at 1375-76.

146. 17 U.S.C. § 1201(a)(1)(A) (2000).

147. *Cf.* Rajani, *supra* note 49, at 376 (discussing essentially the same elements as required for an adequate circumvention analysis, but treating the absence of defenses as an additional element).

that courts have required for § 1201(a)(2) claims yields essentially these same elements,[148] but adds a sixth: (6) that the circumvention "infringes or facilitates infringing a right protected by the Copyright Act," rather than merely allowing noninfringing use of the protected work.[149]

In ruling that StorageTek was likely to prevail on its DMCA circumvention claim,[150] the district court fully considered only two elements: (1) the fact that GetKey was circumvented, and (2) that GetKey was a TPM.[151] The district court did not analyze (3) whether the access control was "effective."[152] Rather, it simply asserted that "GetKey is unquestionably a qualifying access control measure."[153] Nor did the district court clearly identify (4) a work to which GetKey restricted access that was (5) protected by copyright. Although the court stated that GetKey restricted CHE's "ability to access the Event Messages,"[154] it expressly declined to reach the issue of whether Event Messages were protectable under copyright.[155]

Because the First Circuit, from which the case arose,[156] had not construed this portion of the DMCA, the Federal Circuit relied on its own de-

148. *Cf.* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004) (listing the elements required for a § 1201(a)(2) claim); *see also* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 546-50 (6th Cir. 2004) (discussing in turn the importance of a TPM controlling access, the effectiveness of the access controls, the existence of actual circumvention, and that the work in question be protected by copyright).

149. *Chamberlain*, 381 F.3d at 1203; *see also Static Control*, 387 F.3d at 564.

150. Storage Tech. Corp. v. Custom Hardware Eng'g,, Inc., No. 02-12102, 2004 WL 1497688, at *3-4 (D. Mass. July 2, 2004).

151. *Id.* at *4. The failure to adequately address elements of the alleged DMCA violation here echoes the shortcomings of the Eighth Circuit's analysis in Davidson & Associates v. Jung, 422 F.3d 630 (8th Cir. 2005). *See* Rajani, *supra* note 49, at 375-76 (arguing that the Eight Circuit failed to address six elements required for an adequate circumvention analysis).

152. *Id.* at *4.

153. *Id.*

154. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *4. After noting that GetKey is an access control, the district court states that "[GetKey] is designed to prevent precisely what defendants achieved, the modification of the Maintenance Level and consequent ability to access the Event Messages." *Id.* The focus thus seems to be on the conduct prevented, not the *work* protected. Given that the court specifically declined to reach the question of whether Event Messages were protected by copyright, the opinion is unclear as to the identity of the work protected by copyright.

155. *StorageTek I*, No. 02-12102, 2004 WL 1497688 at *3 n.3.

156. The First Circuit typically has jurisdiction over appeals from the District Court of Massachusetts. In this case, StorageTek's complaint contained patent claims, *StorageTek II*, 421 F.3d at 1310, which, although not the subject of appeal, created Federal Circuit jurisdiction. *See* 28 U.S.C. § 1295(a)(1) (2000).

cision in *Chamberlain*, which held that § 1201 only prohibits circumvention that infringes or facilitates infringement of an underlying exclusive right under the Copyright Act.[157] Applying *Chamberlain*, the Federal Circuit stated that the district court erred by not considering whether the circumvention actually facilitated infringement (element (6)).[158] Although the Federal Circuit found no underlying infringement (based both on the § 117(c) theory discussed in Section III.A and an implied license theory, discussed in Section III.C), it stated that even if CHE's RAM copies were unauthorized, StorageTek's DMCA claims would fail because of an insufficient link between rebooting, which caused the copying, and the circumvention of GetKey, which, itself, caused no copying.[159] The fact that the copying of code into RAM and circumvention happened concurrently was insufficient to establish the required nexus between the circumvention and infringement.[160]

StorageTek, by holding that § 1201(a)(1) serves existing rights rather than creating an independent right, applies the reasoning set out in *Chamberlain* and *Static Control* beyond the anti-trafficking provision at issue in those cases to the critical anti-circumvention provision. Thus, in Federal Circuit jurisprudence, this DMCA holding technically breaks new ground by requiring a nexus to infringement as an element of a § 1201(a)(1)(A) claim. Nevertheless, given the broad dicta in *Chamberlain*, this extension is unsurprising and straightforward.

This portion of the decision is remarkable because it again exhibits the theme—also seen in the licensing analysis—that use of a copyright remedy is appropriate only when the underlying wrong violates (or facilitates

157. *StorageTek II*, 421 F.3d at 1307, 1318-19 (discussing Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004)). *Chamberlain* indicated that while § 1201 may be violated without actual infringement of the § 106 rights, some nexus to either infringement or the facilitation of infringement is required. *Chamberlain*, 381 F.3d at 1204. As the court noted, this nonetheless represents a new weapon in the arsenal of the copyright owner: "Prior to the DMCA, a copyright owner would have had no cause of action against anyone who circumvented any sort of technological control, but did not infringe. The DMCA rebalanced these interests to favor the copyright owner; the DMCA created circumvention liability for 'digital trespass' under § 1201(a)(1)." *Chamberlain*, 381 F.3d at 1195-96. The court indicated the limits of this "digital trespass," writing, "circumvention *is not* a new form of infringement but rather a new violation prohibiting actions or products that facilitate infringement." *Chamberlain*, 381 F.3d at 1197 (emphasis in original).

158. *StorageTek II*, 421 F.3d at 1318.

159. *Id.* at 1319.

160. *Id.* Note that the Federal Circuit viewed the maintenance code, rather than the Event Messages, as the work in question.

the violation of) the core rights that copyright protects.[161] In other words, the DMCA exists to help protect copyrighted works,[162] not to create an independent set of rights, nor to help owners of copyrighted works enforce license terms, and certainly not to assist manufacturers in dominating the service market for computer equipment. Thus, this decision rejects the "paracopyright" view of the DMCA discussed in Part I.

2. A New TPM Arms Race?

A legitimate concern after *StorageTek* is whether the Federal Circuit's decision, and the view of the DMCA it reflects, will simply encourage the StorageTeks of the world to employ more powerful TPMs in an attempt to lock ISOs out of the market for equipment service regardless of § 117(c) or legal penalties for the circumvention of TPMs. This effort would be undesirable not only if it succeeded in using TPMs to lock up the service market, but also if it failed after successive generations of TPMs were met with escalating circumvention efforts in an economically wasteful "arms race" between equipment makers and ISOs.

Although this is a danger, there are reasons to expect that the decision will not trigger massive investment in TPMs. First, an arms race is not only undesirable for society, but unattractive for potential participants because of the prospect that even those that invest heavily may lose the race. Second, the continued availability of DMCA liability to reinforce TPMs when actually used to protect the legitimate rights of copyright, which is presumably the majority of cases, limits the need for super-TPMs and lowers the expected return on investment in such TPMs. Third, use of TPMs outside that context might itself be considered anticompetitive behavior, triggering a cause of action under antitrust or unfair competition laws.[163] Fourth, as discussed above, bargaining over license terms would appear to be a much lower-cost, lower-risk approach.

Of course, providing DMCA liability for circumventing TPMs, regardless of underlying infringement, might head off an arms race. But the law is not obliged to avoid an arms race at all costs. On the contrary, the law

161. *Id.* at 1318.

162. *Id.*

163. For instance, using a TPM to tie the right to copy a work, which is one of the § 106 exclusive rights, to the right to use a work might be challenged as an illegal tying arrangement under § 1 of the Sherman Act (15 U.S.C. § 1 (2000)). CHE made an antitrust tying argument in its appellate brief, arguing that StorageTek effectively tied service to its hardware through it licensing terms. But use of TPMs might have a similar anticompetitive effect. Or, use of TPMs to essentially fence-off what the fence-builder does not own might be deemed unfair competition under broad unfair competition statutes. *See, e.g.*, CAL. BUS. & PROF. CODE § 17200 (2007).

should only back up TPMs with circumvention penalties when the law has an interest in protecting that to which the TPMs restrict access. Otherwise the law simply assists parties in putting up fences—regardless of whether they own what is fenced-off.

C. Software Licensing, Agency, and Copyright Liability

This Section considers the holdings of *StorageTek* concerning (1) whether the use of works beyond the scope of a license results in copyright liability, and (2) the circumstances in which a license extends to the licensee's agent.

Like the use of TPMs, the use of restrictive software licensing terms potentially enable licensors to restrict access to or uses of works that would otherwise be allowed under copyright law.[164] The Federal Circuit's discussion of the relationship between license rights and copyright in *StorageTek* exhibits an awareness of the limits of copyright law and the dangers of invoking copyright remedies based on conduct that does not fall within the exclusive rights recognized by copyright law.

Besides claiming the § 117(c) safe harbor, CHE argued that as the agent of StorageTek's licensee (the machine owner), it had a license to copy the maintenance code.[165] StorageTek contended that this argument failed because its licensee's rights were not transferable to CHE, and in any case, the licensee itself had no rights to use the maintenance code.[166] Having found CHE likely to prevail under § 117(c), the court nonetheless reached the license issue, holding both that CHE benefited from an implied license to copy the code into RAM, and that *use* that went beyond the license terms would not give rise to copyright infringement.[167] The Federal Circuit presented this holding as an alternative ground for vacating the district court's preliminary injunction.[168]

---

164. J.H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information*, 147 U. PA. L. REV. 875, 912 (1999) ("Software vendors could . . . override the express exceptions and limitations of copyright law, including the negative rights of users codified in that law and other elements of the statutory 'cultural bargain.'").

165. Non-Confidential Brief of Defendant-Appellants Custom Hardware Engineering & Consulting, Inc. and David York at 28-29, Storage Tech. Corp. v. Custom Hardware Eng'g, Inc., 421 F.3d 1307 (Fed. Cir. 2005) (No. 04-1462), 2004 WL 5003204.

166. *StorageTek II*, 421 F.3d at 1315-16.

167. *Id.*

168. *Id.* at 1317.

1. Contract Liability versus Copyright Liability for Use-Based License Breaches

StorageTek argued that *use* of maintenance functions was expressly prohibited by the license, and thus outside its scope.[169] In response, the Federal Circuit held that *copying* of the maintenance code into RAM was within the scope of the license, and stated that even if CHE's *use* of the maintenance code went beyond the license, since the *copying* was within the scope, StorageTek's claims would sound in contract, not in copyright.[170] In reaching this conclusion, the court distinguished earlier appellate decisions—including one by the First Circuit, whose law it was applying—that suggested that copyright protection extends to all conduct that violates the scope of a license.[171] Examining those decisions, the court found that the unlicensed uses in each case involved acts of copying, such that "those cases thus stand for the entirely unremarkable principle that 'uses' that violate a license agreement constitute copyright infringement only when those uses would infringe in the absence of any license agreement at all."[172]

The approach taken by the court is superficially at odds with the approach taken by the Ninth Circuit in *Arizona Cartridge Remanufacturers Association v. Lexmark International, Inc.*[173] Like *StorageTek*, the *Arizona Cartridge* case concerned a manufacturer attempting to restrict aftermarket competition—namely competition for printer cartridges. In *Arizona Cartridge*, printer cartridge purchasers received an upfront discount (or "prebate") on cartridges in return for an agreement to return them to Lexmark rather than having third parties "remanufacture" the cartridges for reuse.[174] The Ninth Circuit affirmed the district court ruling that this restriction was enforceable, such that using the cartridges product beyond the restrictive terms of the license would be patent infringement.[175]

---

169. *Id.* at 1315.

170. *Id.* at 1316.

171. *Id.* The cases distinguished included S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081 (9th Cir. 1989) (finding infringement where licensee exceeded scope of license by copying and modifying software), and a case from the First Circuit, whose law the Federal Circuit was applying, John G. Danielson, Inc. v. Winchester-Conant Props., Inc., 322 F.3d 26, 40 (1st Cir. 2003) ("Uses of the copyrighted work that stay within the scope of a nonexclusive license are immunized from infringement suits.").

172. *StorageTek II*, 421 F.3d at 1316.

173. Ariz. Cartridge Remanufacturers Ass'n v. Lexmark Int'l, Inc., 421 F.3d 981, 986 (9th Cir. 2005).

174. *Id.* at 983-84.

175. *Id.* at 986-87, 989. Nonetheless, the force of this statement by the Ninth Circuit is unclear. Although the Ninth Circuit affirmed the district court's finding, it stated that

The critical difference between *Arizona Cartridge* and *StorageTek* is that the right to *use* a product is central to patent law, whereas use is *not* one of the exclusive rights granted under the Copyright Act.[176] That use of software is not within the exclusive rights is clear from the legislative history: "Section 102(b) is intended, among other things, to make clear that the expression adopted by the programmer is the copyrightable element in a computer program, and that the actual processes or method embodied in the program are not within the scope of the copyright law."[177] CONTU expressed the same limitation.[178] In short, license violations create copyright liability only when the activity that goes beyond the license is within the § 106 rights.

The Federal Circuit's separation of contract and copyright claims has practical consequences. Remedies available for breach of a software license may be less attractive than the statutory damages and attorney's fees available for copyright infringement. In addition, federal court may be a more attractive venue for plaintiffs in certain cases. Moreover, to enforce its license, a manufacturer such as StorageTek would presumably have to sue its own customer/licensee, which might be an unattractive prospect.

But these consequences, if unattractive to the copyright holder, are nonetheless entirely appropriate. Contract remedies are designed to protect the expectation interests of the contracting parties—in this case Storage-

---

because the issue was not raised by the parties, it would not address the merits of the Federal Circuit case on which this rule was based. *Id.* at 987. *See* Mallinckrodt, Inc. v. Medipart, Inc., 976 F.2d 700, 708 (Fed. Cir. 1992) ("The appropriate criterion is whether [a] restriction is reasonably within the patent grant, or whether the patentee has ventured beyond the patent grant and into behavior having an anticompetitive effect not justifiable under the rule of reason."). Extending this rule to *StorageTek* would support the Federal Circuit's restriction of copyright liability for activity within the "copyright grant."

176. *Compare* 35 U.S.C. § 271(a) (2000) ("[W]hoever without authority makes, uses, offers to sell, or sells any patented invention . . . infringes the patent"), *with* 17 U.S.C. § 106 (2000) (setting forth rights of reproduction, preparation of derivative works, distribution, public performance, and public display).

177. H.R. REP. NO. 94-1476, at 57, *as reprinted in* 1976 U.S.C.C.A.N 5659, 5670 (1976).

178. The CONTU REPORT states:

> Copyright, therefore, protects the program as long as it remains fixed in a tangible medium of expression but not the electro-mechanical functioning of a machine. The way copyright affects games and game-playing is closely analogous—one may not adopt and republish or redistribute copyrighted game rules, but the copyright owner has no power to prevent others from playing the game . . . . Thus one is always free to make a machine perform any conceivable process (in the absence of a patent), but one is not free to take another's program.

CONTU REPORT, *supra* note 19, at 20 (citations omitted).

Tek and its licensee. Copyright should not provide a boon to manufacturers like StorageTek in disputes that do not directly concern the exclusive rights of § 106. Moreover, the inability to get copyright remedies for license violations does not limit a vendor's ability to negotiate terms restricting use, if such terms are mutually advantageous. Agreeable terms might even include stipulated damages provisions in amounts comparable to copyright damages. By limiting such disputes to contract remedies, this decision encourages open negotiation between the parties, which should produce economically efficient outcomes.[179]

2. *The Extension of Software Licenses to ISO Agents*

StorageTek highlighted a license term stating that the licensee/owner could not "sublicense, assign, lease or permit another person to use [StorageTek's] code" as evidence that CHE could not make use of the license at all.[180] Yet the Federal Circuit found that this restriction was unclear in light of other license language expressly allowing the owner to "transfer possession of [the code] only with the transfer of the equipment."[181] The court ruled that:

> Because the whole purpose of the license is to allow the tape library owners to activate their machine without being liable for copyright infringement, such activity by the licensee *and its agents* is implicitly authorized by the license agreement unless the agreement explicitly prohibits third parties from powering up the machines.[182]

The court compared the StorageTek license to more explicitly restrictive licenses in cases, including *Peak*, where ISO activity was held to be outside the scope of the equipment owners' licenses.[183]

The import of this holding is limited insofar as it is tied to the particular license in this case. Yet the holding signals to future licensors that to be effective, license terms prohibiting use by agents must be both explicit and consistent with the license as a whole. Assuming that those conditions were met, the holding indicates such a term would be enforceable. As such, the Federal Circuit's decision amounts to a default rule that agents of a machine owner are authorized to power up the machine, making RAM

179. *See generally* Ronald Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1 (1960).

180. *StorageTek II*, 421 F.3d at 1316.

181. *Id.* at 1316.

182. *Id.* at 1317 (emphasis added).

183. *Id.*

copies of software in the process. As a default rule, it can be contracted around if doing so is in the interests of both parties. Because doing so requires unambiguous language, the term is more likely to come to the attention of an equipment purchaser and thus be the subject of informed bargaining leading to a mutually acceptable outcome. Future purchasers are likely to demand concessions in exchange for giving up the rights to authorize ISOs or other agents to act within the scope of the license.

IV. CONCLUSION: COPYRIGHT LAW AS NEITHER SWORD NOR SHIELD IN THE COMPUTER MAINTENANCE MARKET

In *StorageTek,* the Federal Circuit interpreted section 117(c) of the Copyright Act and section 1201(a)(1) of the DMCA in a manner that respects the competition-promoting purpose of the CMCAA, requires a nexus between DMCA violations and underlying infringement, and reasonably limits the role copyright law plays in the competition between computer equipment makers and ISOs in the computer equipment service market.

The Federal Circuit construed the contours of § 117(c)'s safe harbor broadly, informed by the policy goal of allowing ISOs to compete for computer service with manufacturers. The court's allowance for various actions done "for purposes only of maintenance or repair" is necessary for the safe harbor's existence, and its analysis of software "necessary for activation" is instructive. If the court's focus on eliminating "artificial restraints on companies engaged in legitimate repair and maintenance activities"[184] effectively weakened the requirement that RAM copies are "immediately" destroyed after maintenance, the basic limitations on the safe harbor survive.

In *StorageTek*, as in *Peak,* a manufacturer arguably tried to use (or misuse) copyright to gain an anticompetitive advantage in the after-market for computer service.[185] Indeed, Custom Hardware Engineering (CHE) accused StorageTek of antitrust violations and of misusing copyright to lock CHE out of the maintenance market for StorageTek tape libraries.[186] The Federal Circuit did not reach CHE's misuse or antitrust defenses. But

184. *StorageTek II*, 421 F.3d at 1312.

185. *Id.* at 1310; *cf.* MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 517-19 (9th Cir. 1993) (holding that ISO infringed manufacturer's software copyright by turning on computer for repair).

186. *StorageTek II*, 421 F.3d at 1310; *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3.

its decision suggests concerns that either a narrow reading of § 117(c), an over-broad reading of the DMCA, or the granting of copyright liability for mere license violations would effectively close off the service market to ISOs—concerns similar to those that drove Congress to create § 117(c).[187]

Although passage of the DMCA raised the possibility that computer equipment manufacturers could simply trade the threat of copyright liability for the threat of DMCA liability in order to dominate the service market, the requirement that § 1201(a)(1)(A) violations have a nexus to underlying infringement alleviates this fear and suggests lessons learned from the impact of *Peak*.[188]

However, in *StorageTek*, accusations of anticompetitive conduct ran in two directions. In the eyes of StorageTek and the district court, it was CHE that was probably engaged in anticompetitive behavior—using § 117(c) as a liability shield while piggybacking off of StorageTek's development efforts.[189] Judge Rader's dissent echoes these concerns, stating that "§ 117(c) is not a carte blanche license to use any program loaded into a computer's RAM when the machine is turned on,"[190] and exuding concern that the "court's opinion today destroys copyright protection for software that continually monitors computing machine behavior."[191]

Free-riding by ISOs is a legitimate concern. It would be troubling if the Federal Circuit simply traded anticompetitive practices of equipment manufacturers for anticompetitive practices of ISOs and license violations by the companies that hire them.

Fortunately, the court's ruling does not make § 117(c) into an absolute shield that protects CHE from non-copyright legal claims. In the wake of the decision, companies like StorageTek remain free to bring claims of license breaches, just as they remain free to bring claims of unfair competition. Rather, the Federal Circuit's decision in *StorageTek* channels allegations of license violations and anticompetitive behavior away from copyright law, to be adjudicated within the appropriate realms of contract law and unfair competition laws. Thus, it discourages parties from dressing up such allegations as copyright claims and tying up the Federal courts. The opinion also encourages informed negotiation about service by requiring that language barring ISO service must be clear and unambiguous if it is to be enforceable.

---

187. *See* H.R. REP. NO. 105-551, pt. 1, at 27 (1998) (discussing the goals of the amendments to § 117).

188. *See Chamberlain*, 381 F.3d at 1183-85; *Static Control*, 387 F.3d at 530-31, 553.

189. *StorageTek I*, No. 02-12102, 2004 WL 1497688, at *3.

190. *StorageTek II*, 421 F.3d at 1321 (Rader, J., dissenting).

191. *Id.*

StorageTek establishes 17 U.S.C. § 117(c) as a broad safe harbor from copyright infringement for ISOs, but not an impregnable safe-haven that shelters opportunistic ISOs from legitimate contract claims or unfair competition claims arising from their activities. The decision should effectively discourage use of copyright as either a sword or a shield in the battle between manufacturers and ISOs for the service market—thus helping to set the conditions for a fair fight.