United States Court of Appeals for the Federal Circuit

04-1462

STORAGE TECHNOLOGY CORPORATION
(doing business as Storagetek),

Plaintiff-Appellee,

v.

CUSTOM HARDWARE ENGINEERING & CONSULTING, INC.,

Defendant-Appellant,

and

DAVID YORK,

Defendant-Appellant.

Charles W. Steese, Steese & Evans, P.C., of Denver, Colorado, argued for plaintiff-appellee. With him on the brief was Sandra L. Potter. Of counsel on the brief were Michael D. Broaddus, Perkins Coie LLP, of Seattle, Washington, and Bobbee J. Musgrave, Musgrave & Theis, LLP, of Denver, Colorado. Of counsel were Jerry A. Riedinger, Perkins Coie LLP, of Seattle, Washington, and Mark T. Wasden, of Washington, DC; and Teresa L. Ashmore, Musgrave & Theis LLP, of Denver, Colorado.

Dean L. Franklin, Thompson Coburn LLP, of St. Louis, Missouri, argued for defendants-appellants Custom Hardware Engineering & Consulting, Inc. and David York. Of counsel on the brief were Edwin G. Harvey and Nicholas B. Clifford, Jr., Simon Passanante, PC, of St. Louis, Missouri, and Anthony G. Simon.

Joseph D. Steinfield, Prince, Lobel, Glovsky & Tye, LLP, of Boston, Massachusetts, for defendant-appellant David York.

Appealed from: United States District Court for the District of Massachusetts

Judge Rya W. Zobel

United States Court of Appeals for the Federal Circuit

04-1462

STORAGE TECHNOLOGY CORPORATION
(doing business as StorageTek),

Plaintiff-Appellee,

v.

CUSTOM HARDWARE ENGINEERING & CONSULTING, INC.,

Defendant-Appellant,

and

DAVID YORK,

Defendant-Appellant.

DECIDED: August 24, 2005

Before RADER, SCHALL, and BRYSON, Circuit Judges.

Opinion for the court filed by Circuit Judge BRYSON. Dissenting opinion filed by Circuit Judge RADER.

BRYSON, Circuit Judge.

Storage Technology Corporation ("StorageTek") manufactures automated tape cartridge libraries that can store massive amounts of computer data. The cartridge libraries consist of Library Storage Modules, or "silos," that contain numerous tape cartridges, tape drives for reading the cartridges, and a robot arm for moving the cartridges. Connected to each silo is a Library Control Unit that controls the robotic

mechanisms in the silo and monitors their progress. The individual silos and Control Units are connected via a local area network to a Library Management Unit, which is a computer that can direct and control several silos. To access data from the library, a user sends a request for the data to the Management Unit. The Management Unit then transmits commands to the appropriate Control Unit to find and read the tape cartridge containing the requested data. The Control Unit then sends the data over the network back to the Management Unit.

A central element of this case concerns what occurs when the entire tape library is first turned on. Upon startup, the Management Unit loads executable code, called the "9330 code," from its hard drive into its random access memory ("RAM"). When the Control Unit is powered up, the Management Unit sends other code, called the "9311 code," across the network to the Control Unit, where it is loaded into the Control Unit's memory. Both processes happen automatically, without any action by the library user.

StorageTek's claims in this case stem from the fact that the 9330 and 9311 computer code is copyrighted. StorageTek describes both the 9330 and 9311 code as consisting of two intertwined, but distinct, groups: functional code and maintenance code. While StorageTek never specifies which portions of its copyrighted code fall into each group, it states that the functional code consists of the portions of the computer program that cause the Management Unit and Control Unit to run, while the maintenance code consists of the portions of the program that diagnose malfunctions and maintain the performance of the Management Unit and Control Unit. When StorageTek sells its tape libraries to customers, the company does not sell the software that runs the library. Rather, it only licenses the programs to its customers. The license

covers only the functional code portions of the software, and it specifically excludes the maintenance code. However, StorageTek provides the entire code to the customer. Both the functional and maintenance code are automatically loaded into the RAM of the Control Unit and Management Unit upon startup, and copying the entire code is necessary to activate and run the library.

Custom Hardware Engineering & Consulting, Inc., ("CHE") is an independent business that repairs data libraries manufactured by StorageTek. In order to diagnose problems with the libraries, CHE intercepts and interprets error messages produced by the maintenance code. The error messages are known as fault symptom codes. The fault symptom codes are generated by the Control Unit and are transmitted to the Management Unit over the network within a package of information, called an Event Message. To ensure that the Control Unit is configured to send the fault symptom codes, CHE needs to override a password protection scheme, called GetKey, which was written by StorageTek to disallow certain unauthorized reconfigurations of the maintenance code on the Control Unit. CHE has used two devices to circumvent GetKey. The original device, called a Library Event Manager ("LEM"), was connected to the network between the Control Unit and the Management Unit. The LEM worked by trying different passwords to "crack" GetKey. The LEM then allowed CHE to force the Control Unit to send fault symptom codes over the network after rebooting the Management Unit and Control Unit. CHE has ceased using the LEM in favor of a different device, the Enhanced Library Event Manager ("ELEM"). The ELEM also is attached to the network between the Control Unit and Management Unit. Rather than "cracking" the GetKey password, the ELEM mimics a signal from the Management Unit

to the Control Unit upon rebooting the Control Unit, which causes the maintenance code on the Control Unit to be configured to send the fault symptom codes. CHE then intercepts the Event Messages and interprets the fault symptom codes. Based on the information in those error codes, CHE is able to diagnose and repair the data libraries.

StorageTek brought an action in the United States District Court for the District of Massachusetts against CHE and its president, David York. StorageTek alleged that CHE committed copyright infringement when CHE rebooted and reconfigured its customers' Control Units and Management Units. Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., No. 02-12102-RWZ (D. Mass.). Additionally, StorageTek alleged that CHE violated the anticircumvention provision of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201(a), when CHE circumvented the GetKey protection system to force the customer's Control Unit to transmit error codes. StorageTek also claimed that CHE misappropriated its trade secrets by intercepting the Event Messages, which StorageTek asserts is confidential information. Finally, StorageTek asserted other claims, including an action for patent infringement, that are not at issue in this appeal. In response, CHE counterclaimed, alleging that StorageTek had committed various antitrust violations.

Upon bringing suit, StorageTek asked the district court to issue a preliminary injunction against CHE. After a hearing on the motion, the district court agreed that StorageTek had shown a substantial likelihood of success on the copyright, DMCA, and trade secret claims. Additionally, the court found that the potential losses to StorageTek's business due to CHE's activities were sufficiently great that the balance of hardships favored issuing a preliminary injunction. Finally, the trial court held that

CHE's antitrust counterclaims would likely fail and in any event could not shield CHE from an injunction. The court therefore enjoined CHE from circumventing the GetKey system, intercepting and displaying Event Messages, or causing the copying of the maintenance code on its customers' systems. CHE appeals. Because the issues on appeal are not within our exclusive jurisdiction, we follow the law of the circuit from which this appeal is taken. Glaxo, Inc. v. Novopharm, Ltd., 110 F.3d 1562, 1572 (Fed. Cir. 1997).

I

CHE does not deny that the copyrighted maintenance code is copied into the Control Unit's or Management Unit's RAM when the company reboots its customers' systems. See MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518-19 (9th Cir. 1993). Nor does CHE dispute that the duplication of the maintenance code is outside the explicit grant of StorageTek's software license to its customers. Absent a defense, CHE's actions would constitute copyright infringement. Stenograph L.L.C. v. Bossard Assocs., Inc., 144 F.3d 96, 99 (D.C. Cir. 1998). CHE maintains, however, that its replication of the maintenance code is permissible based on a variety of defenses. Specifically, CHE argues that the copying is protected by sections 117(a) and 117(c) of the Copyright Act, 17 U.S.C. §§ 117(a), 117(c), and the doctrine of fair use. CHE also claims that it is implicitly authorized to copy the maintenance code and that StorageTek's copyright on the code is invalid.

A

CHE first asserts that section 117(c) of the Copyright Act shields it from liability for copyright infringement. Section 117(c) has not previously been construed by the

First Circuit or any court of appeals, and we therefore treat the issue as one of first impression. Section 117(c) provides that

> it 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 activation of a machine that lawfully contains an authorized copy of the computer program, for purpose 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 the machine to be activated, such program or part thereof is not accessed or used other than to make such new copy by virtue of the activation of the machine.

CHE's position is that its actions are protected by section 117(c) because the owners of the tape libraries authorize CHE to turn on the Control Units and Management Units to maintain and repair the tape libraries, and the duplication of the software into RAM is necessary for the machine to function. CHE also argues that its activities fall directly within Congress's purpose in enacting section 117(c), which was to "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." H.R. Rep. No. 105-551, pt. 1, at 27 (1998).

StorageTek contends that CHE's activities fail to meet the requirements of sections 117(c)(1) and 117(c)(2). Specifically, StorageTek claims that CHE does not destroy the copy of the computer code in RAM after the maintenance is completed, in contravention of section 117(c)(1). StorageTek also claims that the maintenance code is not "necessary for the machine to be activated," and that CHE therefore violates section 117(c)(2) when it accesses the maintenance code to diagnose errors in the cartridge library. The dissent agrees.

The requirement in section 117(c)(1) that the new copy of the computer program be destroyed after maintenance or repair is completed can be achieved in most cases by turning off the machine, which erases the copy from RAM. In this case, the evidence showed that CHE reboots the storage libraries at the conclusion of its maintenance contract with the owners of the storage libraries, thus destroying the copy of the computer program in RAM. However, the district court determined that the destruction of the copy at that point does not satisfy the requirements of section 117(c)(1) because CHE "fails to destroy the copies they make immediately after completion of repairs." In other words, the district court looked to whether CHE rebooted the machines each time it repaired a particular malfunction in the silo. The flaw in the court's analysis is that it focuses on the term "repair" in the statute, while ignoring the term "maintenance."

Section 117(d) defines "repair" as "the restoring of the machine to the state of working in accordance with its original specifications . . . ." 17 U.S.C. § 117(d)(2). It defines "maintenance" as "the servicing of the machine in order to make it work in accordance with its original specifications . . . ." 17 U.S.C. § 117(d)(1). Those two definitions make clear that Congress contemplated two distinct activities. The term "repair" denotes fixing a broken machine that is no longer "working in accordance with its original specifications." That term would apply whenever there is a discrete problem with the machine, e.g., when there are "worn or defective components such as memory chips, circuit boards, and hard drives" that need to be replaced. S. Rep. No. 105-190, at 58 (1998). Once the machine is "restored" to its original working condition, the new copy of the program would have to be destroyed immediately in order for section 117(c) to apply. In contrast, the term "maintenance" has a much broader temporal connotation.

The Senate Report on section 117 characterized "maintenance" as including "checking the proper functioning of [ ] components." Id. Thus, maintenance, or "servicing," was meant to encompass monitoring systems for problems, not simply fixing a single, isolated malfunction.

This interpretation of the term "maintenance" comports with the general policy underlying the enactment of section 117(c). That policy was "to 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." H.R. Rep. No. 105-551, pt. 1, at 27. Congress thus sought to protect the class of companies that fix and maintain computer systems, as opposed to those that would make other commercial use of copyrighted material. The point of requiring that copies be "destroyed immediately after the maintenance or repair is completed" was not to create artificial restraints on companies engaged in legitimate repair and maintenance activities, but to prevent persons from invoking the protection of section 117 and then later using the copied material for a prohibited purpose. It would run counter to that objective to construe section 117(c) narrowly to apply only to companies that performed repair in discrete, temporally isolated stages, rather than to construe the statute to apply to repair and maintenance services generally, so long as the companies' only reason for copying the software at issue was to fix and maintain the machines on which the software was running.

In its analysis of section 117(c), the district court gave considerable weight to the testimony of StorageTek's expert, Christian Hicks. The court noted that Mr. Hicks testified that a copy of the copyrighted software program remains in the Management

and Control Units' RAM on an ongoing basis as the system operates with the LEM or ELEM attached. Because that description did not comport with the notion of "repair," the court held section 117(c) inapplicable. In describing CHE's process, however, Mr. Hicks noted that "the LEM and ELEM stay in place at the facilities so that when problems occur," CHE can detect and fix the malfunction. That is the same as saying that while the LEM and ELEM are attached, CHE "checks the proper functioning" of the storage library and ensures that the machine "works in accordance with its original specifications." Accordingly, CHE's actions fall within the definition of maintenance in section 117. Moreover, when CHE's maintenance contract is over, CHE stops its maintenance and immediately reboots the storage library, thereby destroying the copy of the copyrighted program. CHE's actions therefore appear to comply with the requirement of section 117(c)(1). While CHE may actively check to ensure that the silo is free from errors over an extended period of time, the protection of section 117 does not cease simply by virtue of the passage of time. Rather, it ceases only when that maintenance ends.

In the alternative, StorageTek contends that CHE cannot avail itself of section 117(c) because the statute requires that "with respect to any computer program or part thereof that is not necessary for the machine to be activated, such program or part thereof is not accessed or used . . . ." According to StorageTek, the maintenance code is "not necessary for the machine to be activated," and CHE's access to and use of the maintenance code to generate the Event Message signal therefore makes CHE liable for infringement. That assertion turns on the meaning of "maintenance code." StorageTek's license agreement states that the maintenance code is software "which

detects, records, displays and/or analyzes malfunctions in [the] Equipment." Because those processes are distinct from "activating the machine," StorageTek argues that duplication of the maintenance code is not covered by section 117(c).

Unfortunately, determining whether a particular piece of software is "necessary for the machine to be activated" is not as simple as it might appear. On the one hand, not all code that resides in a machine's RAM after the completion of the startup routine qualifies as "necessary for the machine to be activated," even though that code is put into RAM as part of the activation process. If that were so, the requirement of section 117(c)(2) would effectively be read out of the statute, since under that interpretation there would be no program that was copied by virtue of activation but could not otherwise be accessed or used. At the same time, the code "necessary for the machine to be activated" cannot be the minimal amount of code that, when loaded into RAM, causes the machine to produce any response. For instance, the programs and drivers that allow the monitor on a personal computer to function do not fall outside the protection of section 117(c) simply because the computer itself can be activated and can function without a monitor attached. If section 117(c) were read that restrictively, accessing copyrighted software that controlled the monitor would put parties at risk of infringement, which would thwart Congress's desire to ensure "that an independent service provider may turn on a client's computer machine in order to service its hardware components." S. Rep. No. 105-190, at 57.

In enacting section 117(c), Congress gave some indication of what it considered to be "necessary for the machine to be activated." Specifically, the House Report on section 117(c) noted 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." H.R. Rep. No. 105-551, pt. 1, at 28. As examples of software that need not be loaded in order for the machine to function, the Report listed programs marketed as separate products that load into RAM along with the operating system or software that the owner of the machine has independently configured the computer to load during initialization. Id. Therefore, separate "freestanding programs" that load into RAM upon startup clearly may not be accessed under section 117(c)(2).

Congress's clearest indication of what it considered to be "necessary for the machine to be activated," however, is found not in section 117(c), but in section 117(d). As we have noted, section 117(d) defines repair and maintenance in terms of allowing the system to work "in accordance with its original specifications and any changes to those specifications authorized for that machine." Thus, 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." Accessing software programs, such as freestanding diagnosis and utility programs, that are not needed to boot up the computer and make that determination, goes too far because access to those programs is not strictly necessary to verify that the computer is "working in accordance with its original specifications."

In some instances, it may be difficult to determine whether particular software is necessary to make the computer function and to ascertain whether the computer is working properly. In this case, however, both parties agree that the maintenance code is so entangled with the functional code that the entire code must be loaded into RAM for the machine to function at all. That is, loading the maintenance code into RAM is

necessary for the Management or Control Unit "to be turned on." Contrary to the dissent's position, the fact that the maintenance code has other functions, such as diagnosing malfunctions in the equipment, is irrelevant. Moreover, the possibility that StorageTek could have written the maintenance code as a separate, "freestanding" program that would not have been needed to start the machine does not affect the statutory analysis of the system that StorageTek in fact created. Finally, although the maintenance code can be reconfigured to perform fewer functions, as the dissent points out, what StorageTek can do with the maintenance code after the system boots up is irrelevant. As the statutory text and legislative history make clear, the phrase "necessary for the machine to be activated" refers to the portion of code that must be copied in order for the machine "to be turned on." In this case, copying the maintenance code into RAM is indispensable for the machine to be turned on or activated; its functionality (or lack thereof) after bootup is moot.

Finally, StorageTek contends that section 117(c) does not apply to CHE's conduct because CHE does not reboot the machine and make a copy of the copyrighted code "for purpose only of maintenance or repair." Specifically, StorageTek maintains that CHE reboots the machine in order to circumvent GetKey and gain access to the fault symptom codes. That argument is unconvincing because CHE's entire purpose in obtaining the fault symptom codes is to diagnose and repair the silos. StorageTek's argument that CHE's activity is not "for purpose only of maintenance or repair" is akin to suggesting that it would be impermissible to activate a keyboard on a personal computer for the purpose of maintenance or repair because the real purpose of activating the keyboard would be to allow the user to type. That line of reasoning, if

accepted, would quickly destroy the protection that section 117(c) affords. 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 maintenance 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." In sum, we conclude that CHE is likely to prevail on the merits of its argument that section 117(c) protects its act of copying of StorageTek's maintenance code into RAM.

B

CHE argues in the alternative that even if the section 117(c) defense is unavailable, CHE is not liable for copyright infringement because it enjoys the benefits of its customers' licenses to copy StorageTek's 9330 and 9311 code in order to activate their machines. StorageTek's license agreement with its customers allows the customers to copy StorageTek's software into RAM "for the sole purpose of enabling the specific unit of Equipment for which the Internal Code was provided to perform its data storage and retrieval or other operating functions." Therefore, the customers do not commit infringement merely by activating their Management and Control Units and consequently copying StorageTek's software into RAM. As an agent of those storage library owners, CHE also does not commit copyright infringement simply by turning on the owners' machines. See Hogan Sys., Inc. v. Cybersource Int'l, Inc., 1997 WL 311526, at *4 (N.D. Tex. June 2, 1997), aff'd, 158 F.3d 319 (5th Cir. 1998) (although the license at issue did "not specifically authorize a third-party consultant to use, copy, or modify Umbrella software," the court found that while the defendants "are engaged in

consulting services on behalf of Norwest, Defendants' activities are 'sheltered under' Norwest's license rights").

StorageTek argues that CHE's use of the maintenance code must constitute infringement because the license agreement specifically excludes the use of the maintenance code. Because CHE's customers are not allowed to access the maintenance code, StorageTek asserts that when CHE does so, it must be infringing StorageTek's copyright. There are two flaws in that line of reasoning. First, CHE's customers are given the right to copy the maintenance code into the RAM of their machines. The license specifically authorizes the customers to use the code to "enabl[e] the specific unit of Equipment." The parties are in agreement that both the maintenance code and functional code portions of the 9330 or 9331 code must be loaded into RAM in order to activate the Control and Management Units. In order to activate the Control and Maintenance Units, the maintenance code must be copied. The license thus authorizes the copying of that code.

Second, StorageTek's argument conflates a claim based on copyright infringement and an action based on breach of contract. To succeed in a copyright action, "the copying must be beyond the scope of a license possessed by the defendant," Stenograph, 144 F.3d at 99, and the source of the copyright owner's complaint must be grounded in a right protected by the Copyright Act, such as unlawful reproduction or distribution. See 17 U.S.C. § 106. In contrast, the rights granted by contract can be much broader. As an example, consider a license in which the copyright owner grants a person the right to make one and only one copy of a book with the caveat that the licensee may not read the last ten pages. Obviously, a licensee who

made a hundred copies of the book would be liable for copyright infringement because the copying would violate the Copyright Act's prohibition on reproduction and would exceed the scope of the license. Alternatively, if the licensee made a single copy of the book, but read the last ten pages, the only cause of action would be for breach of contract, because reading a work does not violate any right protected by copyright law. Likewise, in this case, the copying of the maintenance code is permitted by the license. The use of the code may violate the license agreement, but it is not forbidden by copyright law and cannot give rise to an action for copyright infringement. See United States Naval Inst. v. Charter Communications, Inc., 936 F.2d 692, 695 (2d Cir. 1991) ("[a] licensee of any of the rights comprised in the copyright, though it is capable of breaching the contractual obligations imposed on it by the license, cannot be liable for infringing the copyright rights conveyed to it").

Although there is language in some cases that can be read to suggest that copyright protection extends to all conduct that would violate the user's license, the decisions in those cases are not that broad. For example, in S.O.S., Inc. v. Payday, Inc., the Ninth Circuit stated that a "licensee infringes the owner's copyright if its use exceeds the scope of its license." 886 F.2d 1081, 1087 (9th Cir. 1989). In that case, however, it was clear that the "use" the copyright owner was complaining about was the defendant's "copying and modification of the software." Id. at 1085. Similarly in John G. Danielson, Inc. v. Winchester-Conant Props., Inc., 322 F.3d 26, 41 (1st Cir. 2002), the First Circuit noted that "[u]ses of the copyrighted work that stay within the scope of a nonexclusive license are immunized from infringement suits." Not only did the court not state that "uses" that fall outside the scope of the license would necessarily constitute a

copyright violation, but the allegedly unlawful "use" in that case was the copying of architectural plans. Id. at 32; see Data Gen. Corp. v. Grumman Sys. Support Corp., 36 F.3d 1147, 1167 (1st Cir. 1994). In light of their facts, 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.

StorageTek maintains that regardless of the scope of its licenses vis-à-vis the equipment owners, the licenses do not extend rights to third parties. In particular, StorageTek points to the language of its standard license agreement, which states that the equipment owner may not "sublicense, assign, lease or permit another person to use Internal Code (except as provided . . . below)." The company argues that this provision forbids CHE from copying StorageTek's code into RAM by starting up the Control and Management Units. That argument, however, ignores the rest of the license agreement. The prohibition on third-party use of the code is modified by a later provision stating that equipment owners "may transfer possession of Internal Code only with the transfer of the Equipment on which its use is authorized." Additionally, the license grants the customer the use of the code for "the sole purpose of enabling the specific unit of Equipment for which the Internal Code was provided . . . ." The clear implication of those sections is that the license is tied to the piece of equipment on which the software resides. Thus, the authorized use is tied to a particular machine, rather than a particular person. In fact, one version of StorageTek's license agreement expressly contemplates third-party use of the equipment, noting that "misuse of the Equipment or negligence by Customer or a third party" is not included within the

maintenance provision of the license. Thus, the prohibition against assigning or permitting another to use the code is clearly a restriction on giving a third party a copy of the code that is divorced from the machine "on which its use is authorized." In this case, CHE is merely turning on the machine on which the use of the code is authorized. See Green Book Int'l Corp. v. Inunity Corp., 2 F. Supp. 2d 112, 116 n.1 (D. Mass. 1998) (multiple individuals may use computer under a license, "which limits use to 'only one single-user computer,' without any additional restriction on the identity of the person who, from time to time, physically sat at and operated such computer"). Because the whole purpose of the license is to allow the tape library owners to activate their machines 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.

Other cases involving software license agreements support that reading of StorageTek's agreement, albeit indirectly. For example, in MAI Systems, the Ninth Circuit held that a third party was not authorized to copy licensed software into RAM by activating a computer. However, the court held that the license did not cover such copying because the license prohibited third parties from copying the software. 991 F.2d at 517. The license in MAI Systems was so restrictive that only three employees of the licensee were allowed to use and copy portions of the software. Id. at 517 n.3. It was only because the license contained such severe, explicit restrictions that the court held that third parties were prohibited from copying the software by activating the machine. The court in MAI Systems would not have had to rest its decision on those restrictive license terms if third parties were disallowed from copying the software even

in the absence of such restrictive language in the license. See also SMC Promotions, Inc. v. SMC Promotions, 355 F. Supp. 2d 1127, 1132 (C.D. Cal. 2005) (forbidding third-party copying by relying on the explicit language of the license, which stated that licensees "may not delegate or authorize any other person to do so, whether on [the licensees'] behalf or otherwise").

StorageTek, of course, could have drafted the license agreement to explicitly disallow copying by third parties through activation of the equipment owners' machines. In the absence of such language, however, CHE's copying appears to be protected as long as CHE is acting as an agent of the equipment owners.

C

In conclusion, the district court erred in finding that CHE was unlikely to prevail on its defense to copyright infringement. CHE's conduct appears to fall within the safe harbor of 17 U.S.C. § 117(c). Additionally, CHE is likely to prevail on its contention that StorageTek's license agreement with its customers allows CHE, as the customers' agent, to copy StorageTek's software into RAM during the activation of the customers' tape libraries. Having concluded that CHE is likely to prevail on the issue of copyright infringement based on section 117(c) and the customers' licenses, we do not need to address CHE's defenses premised on section 117(a), fair use, and invalid registration.

II

The DMCA claim is based on CHE's circumvention of the GetKey protocol. Specifically, StorageTek maintains that the use of the ELEM and LEM devices violates section 1201(a)(1) of title 17 of the United States Code, which prohibits any person from "circumvent[ing] a technological measure that effectively controls access to a work

protected under this title." While the First Circuit has not addressed the scope of the DMCA's prohibition under section 1201(a), this court has confronted the issue in Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004).

In Chamberlain we held that when Congress enacted the DMCA, it "chose to create new causes of action for circumvention and for trafficking in circumvention devices. Congress did not choose to create new property rights." 381 F.3d at 1203. Accordingly, we held that section 1201 "prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners." Id. at 1202. A copyright owner alleging a violation of section 1201(a) consequently must prove that the circumvention of the technological measure either "infringes or facilitates infringing a right protected by the Copyright Act." Id. at 1203.

In this case, the LEM and ELEM devices allow CHE to bypass GetKey and gain access to the maintenance code. Furthermore, the manner in which the ELEM and LEM function requires that the Control or Management Units be rebooted, causing the protected software to be copied into RAM. Nonetheless, simply because the ELEM or LEM allows access to the copyrighted work concurrently with the copying does not mean that the ELEM or LEM "facilitates" copyright infringement. Consequently, the district court erred by failing to consider whether or not such facilitation occurred.

We held above that it is unlikely StorageTek will succeed on the merits of its copyright claim. To the extent that CHE's activities do not constitute copyright infringement or facilitate copyright infringement, StorageTek is foreclosed from maintaining an action under the DMCA. See Chamberlain, 381 F.3d at 1202. That

result follows because the DMCA must be read in the context of the Copyright Act, which balances the rights of the copyright owner against the public's interest in having appropriate access to the work. See id. at 1199 ("the severance of access from [copyright] protection . . . would also introduce a number of irreconcilable problems in statutory construction"); 17 U.S.C. § 1201(c)(1) ("Nothing in this section shall affect rights, remedies, limitations, or defense to copyright infringement . . . ."); see also Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984). Therefore, courts generally have found a violation of the DMCA only when the alleged access was intertwined with a right protected by the Copyright Act. See, e.g., Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943, 987 (E.D. Ky. 2003), vacated and remanded on other grounds, 387 F.3d 522 (6th Cir. 2004); RealNetworks, Inc. v. Streambox, Inc., 2000 WL 127311, at *7 (W.D. Wash. Jan. 18, 2000); accord Universal City Studios v. Corley, 273 F.3d 429, 435 (2d Cir. 2001) (explaining that Congress enacted the DMCA to help copyright owners protect their works from piracy). To the extent that StorageTek's rights under copyright law are not at risk, the DMCA does not create a new source of liability.

Even if StorageTek were able to prove that the automatic copying of the software into RAM constituted copyright infringement, however, it would still have to show that the LEM or ELEM facilitated that infringement. See Chamberlain, 381 F.3d at 1202. If such a nexus were not required, the careful balance that Congress sought to achieve between the "interests of content creators and information users" would be upset. See H.R. Rep. No. 105-551, pt. 1, at 26.

The problem in this case is that the copying of the software into RAM when the Control or Management Units are rebooted takes place regardless of whether the LEM or ELEM is used. Hence, there is no nexus between any possible infringement and the use of the circumvention devices. Rather, CHE's circumvention of GetKey only allows CHE to use portions of the copyrighted software that StorageTek wishes to restrict technologically. The activation of the maintenance code may violate StorageTek's contractual rights vis-à-vis its customers, but those rights are not the rights protected by copyright law. There is simply not a sufficient nexus between the rights protected by copyright law and the circumvention of the GetKey system.

A court must look at the threat that the unauthorized circumvention potentially poses in each case to determine if there is a connection between the circumvention and a right protected by the Copyright Act. See Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 549-50 (6th Cir. 2004); Chamberlain, 381 F.3d at 1204. In this case, the threat from CHE's circumvention of GetKey is distinct from the dangers that StorageTek's copyright protects against. See 17 U.S.C. § 106.

In sum, the district court failed to consider whether the circumvention of the GetKey system either infringes or facilitates infringing a right protected by the Copyright Act. We conclude that it is unlikely that StorageTek will prevail on its claim under section 1201(a) in this case because the ELEM and LEM devices are not reasonably related to any violation of the rights created by the Copyright Act.

III

StorageTek asserts that the information contained in the Event Messages constitutes a trade secret. Accordingly, StorageTek contends that by breaking GetKey

and reconfiguring the Control Units to send the Event Messages, CHE has misappropriated the secret information contained in the Event Messages. StorageTek's argument is undermined, however, by the fact that the pertinent information in the Event Messages used to be publicly available.

Trade secret protection is unavailable for information that is not actually secret. See Jet Spray Cooler, Inc. v. Crampton, 282 N.E.2d 921, 925 (Mass. 1972). Therefore, information that is in the public domain cannot be appropriated by a party as its proprietary trade secret. CVD, Inc. v. Raytheon Co., 769 F.2d 842, 850 (1st Cir. 1985) ("Once a trade secret enters the public domain, the possessor's exclusive rights to the secret are lost."). While StorageTek took precautions to protect the information in the Event Messages by implementing GetKey, those efforts are insufficient to create trade secret rights if the public previously had access to the information contained in the Event Messages.

CHE maintains that the vital information in the Event Messages—the meaning of the fault symptom codes—was public knowledge before StorageTek created GetKey. There appears to be overwhelming evidence that the fault symptom codes were freely transmitted by the library components, with no effort to keep their meaning secret. StorageTek's senior customer service engineer testified that the fault system codes were not confidential. That fact was confirmed by CHE's expert. There was even evidence that early versions of StorageTek's software would cause the error codes to be shown on the Control Unit's display panel whenever there was an error. In fact, technicians first learned the meaning of the error messages by recording the error message that was revealed on the display panel for each type of machine malfunction.

There was also evidence that the entire Event Message was openly transmitted before the GetKey system was put in place. Mr. Billington, StorageTek's expert, testified that from 1987 until 1992 the data packets were "freely available."

StorageTek makes two arguments in support of its contention that the Event Messages were never freely available. First, it maintains that in 1992, before GetKey was implemented, StorageTek attempted to keep the error codes secret by disabling the maintenance code, which sends the Event Messages, on customers' machines. Those actions are irrelevant, however, because the error messages had already been freely transmitted between 1988 and 1992. See J.T. Healy & Son, Inc. v. James A. Murphy & Son, Inc., 260 N.E.2d 723, 730 (Mass. 1970) (a trade secret is lost when the owner "lie[s] back and do[es] nothing to preserve its essential secret quality"). Second, StorageTek argues that it is immaterial that the general meaning of the fault symptom codes was in the public domain. Instead, StorageTek contends that the pertinent confidential information is the error message corresponding to a specific customer's equipment malfunction. Thus, according to StorageTek, the secret information is the error message that would be sent by a particular customer's machine if the machine were configured to produce and transmit fault symptom codes. Given that the general meanings of the fault symptom codes are in the public domain, however, that argument seemingly implies that the actual error on the customer's machine is secret. Yet the machines are owned by the customer and are in the customer's possession. The reason that the machine is malfunctioning therefore cannot possibly be considered a secret. As an analogy, consider a stock broker who devised a program that would notify him when a stock price was at a point at which the stock was worth buying. Obviously

that special "buy price" could be a trade secret if it had not been previously made public, but in no event could the actual market price that triggered the notification be considered a trade secret. Similarly, the meaning of the fault symptom codes might have been a trade secret if they had not been previously made public, but the actual reason for the machine malfunctioning would not be.

The dissent maintains that "the information detailing precisely which aspect of the system is broken and how to fix it" is protected as a trade secret. However, as we have noted, the meanings of the codes and the malfunction itself are public information. Additionally, there is no indication that the Event Messages provide a prescription of how to fix the machine rather than simply a diagnosis of what is wrong. The dissent further claims that trade secrets "remain trade secrets unless and until a third party discovers the information on its own." That analysis fails for two reasons. First, the owner of the trade secret bears the burden of taking reasonable steps to preserve the secrecy of the trade secret. See USM Corp. v. Marson Fastener Corp., 393 N.E.2d 895, 899-900 (Mass. 1979). The dissent's position apparently shifts the burden onto others to discover the trade secret information independently. Second, to show misappropriation of a trade secret under Massachusetts law, StorageTek must show that CHE "used improper means, in breach of a confidential relationship, to acquire and use the trade secret." Data Gen., 36 F.3d at 1165. CHE uses publicly available information about what the fault symptom codes mean, and it developed the LEM and ELEM devices independently to diagnose problems in the silos. There has been no showing that either of those activities breached a confidential relationship. Therefore, the diagnostic information obtained through those methods, i.e. determining what is

physically wrong with the silo, cannot be a misappropriation of a trade secret, any more than if CHE had reverse engineered the silo in any other manner. Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 160 (1989).

For these reasons, we agree with the appellants that the district court erred in failing to consider whether the information contained in the error messages is secret. Because it appears that the information for which StorageTek asserts trade secret protection was previously in the public domain, we conclude that StorageTek is unlikely to prevail on the merits of its trade secret claim.

IV

Because the district court committed errors of law in its consideration of StorageTek's copyright claim and because the district court overlooked material factors in its analysis of the DMCA and trade secret claims, we find the court abused its discretion in granting the preliminary injunction. See Bl(a)ck Tea Soc'y v. City of Boston, 378 F.3d 8, 11 (1st Cir. 2004). Therefore, we vacate the grant of the preliminary injunction and remand for further proceedings.

VACATED and REMANDED.

United States Court of Appeals for the Federal Circuit

04-1462

STORAGE TECHNOLOGY CORPORATION
(doing business as Storagetek),

Plaintiff-Appellee,

v.

CUSTOM HARDWARE ENGINEERING & CONSULTING, INC.,

Defendant-Appellant,

and

DAVID YORK,

Defendant-Appellant.

RADER, Circuit Judge, dissenting.

This court's opinion today destroys copyright protection for software that continually monitors computing machine behavior. The opinion also conflates methods used to protect trade secret information with the actual information constituting the trade secret. Because these holdings are contrary to the underlying law, I respectfully dissent.

The safe harbor created by § 117(c) is not a carte blanche license to use any program loaded into a computer's RAM when a machine is turned on. Section 117(c)(2) specifically precludes a repairman from using copies of programs loaded into RAM upon powering-up that are "not necessary for that machine to be activated." Maintenance code that continually monitors for faults, as does Storage Tek's, is loaded into RAM upon powering-up the system but, as CHE admits, the maintenance code can be disabled with no affect on the operating aspects of the system. Of course, disabling the

maintenance code eliminates continuous monitoring for faults. Even though Storage Tek has chosen to load the maintenance code upon activation, the maintenance code as such is incidental, not indispensable, to activation. Consequently, CHE's use of copies of Storage Tek's maintenance code falls outside the safe harbor created by § 117(c).

This court's opinion holds that CHE's copying and use of Storage Tek's diagnostic "maintenance code" software falls within the protection of § 117(c) because "CHE 'checks the proper functioning' of the storage library and ensures that the machine 'works in accordance with its original specifications.'" However, § 117(c) places restrictions upon the use of maintenance software. Therefore, while I agree that "maintenance" includes checking the proper functioning of components, I do not agree that CHE's use of Storage Tek's maintenance code falls within the protection of § 117(c).

When using Storage Tek's maintenance code, which is not code "necessary for the machine to be activated," CHE does not reboot the storage silos of its clients for the sole purpose of making a new copy "by virtue of the activation of the machine." If it did, CHE would be within the safe harbor of § 117(c). Although at the time CHE reboots it repairs nothing, adjusts nothing, and checks nothing, CHE subsequently accesses and uses the maintenance code to send data packets that indicate the operation of the system. Therefore, CHE does not fall within the safe harbor of § 117(c)(2).

Alternatively, even if Storage Tek's maintenance code were so written as to be "necessary for the machine to be activated," when CHE reboots the silos with that code, it once again repairs nothing, adjusts nothing, and checks nothing. Because CHE does

not perform any “maintenance” or “repair” when it reboots the system to manipulate the maintenance code, this copying of the maintenance code does not fall within the protection of § 117(c)(1).

Section 117(c) allows a repairman to turn on a machine and to use the programs necessary to run the machine for the limited period of time the repairman is actually working on the machine, whether the repairman is fixing something that is actually broken, or servicing parts to prevent the machine from breaking in the future. Servicing parts may certainly encompass “putting the machine through the paces” to ensure that all the parts are properly functioning. In other words, the words “maintenance” and “repair” in § 117(c) extend the protection of § 117(c) to cover both the monitoring of function to assure that repair is not needed, and identification of malfunction to facilitate repair. However, the “maintenance and repair” must be of limited duration. Section 117(c)(1) specifies that any copy of the maintenance software must be destroyed “after the maintenance or repair is completed.” CHE, however, does not meet this condition. CHE runs the maintenance software continually to monitor operation. Only when a problem arises during monitoring, does CHE actually work on the silo. Thus, CHE uses the copy of the maintenance code in RAM beyond actual servicing or repairing. This continual use falls outside the scope of § 117(c).

As this court’s opinion states, the policy of § 117(c) is “to 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. . . . The point of requiring that copies be ‘destroyed immediately after the maintenance or repair is completed’ was not to create artificial restraints on

companies engaged in legitimate repair and maintenance activities, but to prevent persons from invoking the protection of § 117 and then later using the copied material for a prohibited purpose." CHE, however, does not boot the machine in order to service or repair it; it boots to manipulate the maintenance level of the maintenance code so that it may read fault codes. As noted above, this is not "maintenance" or "repair" under § 117(c). CHE also does not "immediately destroy" the copy when the service or repair is completed. CHE uses the maintenance code even while the machine is functioning properly and is in full use by the client. How can CHE's continual use of Storage Tek's software during a three-year (or more) contract not be "using the material for a prohibited purpose"? Again, the "immediately destroy" requirement of § 117(c) protects use only during the limited time the repairman is actually working on the computer.

This court also holds that the diagnostic information contained in the data packets created and sent by the maintenance code cannot be a trade secret because "the reason the machine is malfunctioning [ ] cannot possibly be considered a trade secret." But it is the data packets themselves, not the physical operation (or mis-operation) that they describe, that is the trade secret. A malfunction may be independently discoverable, but that does not preclude the information which describes it from being a trade secret. In my eyes, this court's analogy to a special "buy price" is flawed. As I see it, the message that the arm of a storage silo is "broken" is analogous to the "buy price" that this court states "cannot possibly be considered a trade secret." The diagnostic information contained in the data packets, i.e., the information detailing precisely which aspect of the system is broken and how to fix it, is analogous to the information detailing why the "buy price" makes a good buy. That a third party may

perform its own diagnostics on the broken system and discover the cause of the malfunction does not remove the proprietary nature of the information until the third party actually performs the diagnostics and discovers the malfunction. Trade secrets remain trade secrets unless and until another party discovers the information on its own, at which point the information enters the public domain and is no longer protected. The point is that the other party must perform the work to discover the information on its own instead of stealing the information from its competitor.

Finally, this court's suggestion that the meaning of the fault symptom codes themselves may have been a trade secret if they had not been introduced into the public domain misses the point. The proprietary fault symptom codes are the language used to express the faults, so it is the correlation of fault and code that forms the lexicon by which the trade secret can be deciphered.

For the foregoing reasons, I respectfully dissent.