UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CIVIL ACTION NO. 02-12102-RWZ

STORAGE TECHNOLOGY CORPORATION
d/b/a STORAGETEK

v.

CUSTOM HARDWARE ENGINEERING &
CONSULTING, INC., and DAVID YORK

MEMORANDUM OF DECISION

July 2, 2004

ZOBEL, D. J.

Plaintiff, Storage Technology Corporation ("StorageTek"), has devised and sells systems for storing and retrieving very large and extensive amounts of computer data. The systems consist of hardware, software and Library Storage Modules installed at customers' sites and connected to computers that control the operation of the modules. Plaintiff also services the customers' installations by means of diagnostic software, the "Maintenance Code," which it uses to identify malfunctions and problems in the customers' storage system. Although the storage systems are programmed with the Maintenance Code along with the functional operations software, the Code is not sold, and only plaintiff has access to it. Plaintiff has copyright registration certificates for virtually all versions of its Maintenance Code and has taken great pains to protect access thereto with a proprietary algorithm it calls a GetKey. Nonetheless, plaintiff charges, defendants have circumvented its security measures and are using the Maintenance Code in their business

as a third-party service provider for plaintiff's systems.[1] It claims that defendants thereby infringe its copyrights, violate the Digital Millennium Copyright Act of 1998, Pub. L. 105-304, codified in relevant part at 17 U.S.C. § 1201 et seq., and unlawfully use its trade secrets.[2] The case is now before me on plaintiff's motion for a preliminary injunction.

At the hearing on the motion, both parties adduced the testimony of witnesses and submitted a number of affidavits; they also filed extensive briefs and proposed orders. They are in substantial agreement as to the requisites for the issuance of a preliminary injunction, namely, a showing of 1) a substantial likelihood of success on the merits, 2) irreparable harm, 3) greater injury to plaintiff from the denial of the injunction than harm to defendant from the granting thereof, and 4) benefit to the public interest. Charlesbank Equity Fund II v. Blinds to Go, Inc., 370 F.3d 151, 162 (1st Cir. 2004). Although the parties contest the precise contours of these requisites as applied in this case, they do agree that the decisive question is whether plaintiff has adequately established the likelihood of success on the merits. If that question is answered affirmatively, irreparable harm is presumed, the weighing of harms to the respective parties is resolved in favor of the copyright holder and, almost by definition, the public interest is best served by upholding copyright protections. Concrete Machinery, Co., Inc. v. Classic Lawn Ornaments, Inc., 843

---

[1]The only defendants implicated in the instant motion are Custom Hardware Engineering & Consulting , Inc. and David York. Three other defendants have only recently been brought into the litigation, and no evidence tied them to copyright and/or trade secret violations.

[2]The Third Amended Complaint in fact includes a number of other counts, and defendants, in addition to denying all allegations of wrongful conduct, have counterclaimed and asserted affirmative defenses of antitrust violations, misuse of copyright and laches. However, in its motion for a preliminary injunction, plaintiff relies only on the claims set forth above.

F.2d 600, 611-12 (1st Cir. 1988).

The following description of plaintiff's system and defendants' circumvention techniques constitutes my findings of fact. Indeed, the parties' evidence presents little divergence of facts – their disagreement concerns largely the characterization and interpretation of those facts.

Plaintiff's storage systems are, at their most basic, a large number of tape libraries that plaintiff collectively calls Silo Systems. They have three components: 1) a Library Storage Module, 2) a Library Control Unit, and 3) a Library Management Unit. The first is a very large box-like structure (14' x14' x 8') and a piece of hardware with robotics that is operated by software in the Control and Management units. It typically contains thousands of tapes, tape drives and a robotic arm to store and retrieve tapes as directed.

The Management Unit is the computer that coordinates an entire system and communicates among its several parts. It receives job requests, usually many at the same time, from the several host computers. Then, based on priorities and availability of robotic hardware, it determines the order in which the jobs are to be completed, and issues commands to the multiple Control Units to produce orderly completion of the jobs. Each Management Unit can operate up to 24 Control Units, each of which, in turn, runs one Storage Unit.

The Control Units are computers that send commands to the robotic mechanisms in the Storage Modules and then monitor their effectiveness. The Control Unit receives its commands from the Management Unit; after receipt it instructs the robots to carry out the assigned task and sends back to the Management Unit a completion report.

Plaintiff has written the software for the operation of the Management and Control Units, designated Functional Code, and for the maintenance of the entire system, designated Maintenance Code. When activated, the latter runs a series of diagnostic tests, provides information as to the nature of the problem and where in the system difficulties have occurred or are likely to blossom, and performs other maintenance-specific operations. It is programmed to be set at different levels between 0 and 9. At 0, the "at rest" and usual setting, the Maintenance Code is disabled, although the system continues to operate normally. Above 0 the Maintenance Code activates specific diagnostic functions at different levels. Among the most important of these are Control Unit event logging, Management Unit event logging and the SAE event log environment user interface. These are the functions that concern the generation, transmittal, storage and display of Event Messages that are triggered as a result of the detection and interpretation of faults or malfunctions in the robotic operations. The Event Messages translate the data readings generated by the diagnostic software into text messages in English that a service technician can read.

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. The Maintenance Code is specified as either 9330 or 9311 in the copyright registration certificates. Plaintiff holds the GetKey algorithm source code in a secure location at its headquarters in Louisville, Colorado. To enable the Maintenance Code for a particular Management Unit, plaintiff's technician must contact plaintiff's technical support

staff, identify him or herself, provide the serial number of the equipment being serviced and identify the desired level of Maintenance Code. This process will yield a GetKey password specific to this request that the technician must enter into the Management Unit. He or she then reinitializes all the units to reset the Maintenance Level. During the process of accessing the Maintenance Code and changing the level, a complete copy of the 9311 Code and a virtually complete copy of the 9330 Code is made in the Management Unit. As the diagnostic work proceeds, specific blocks of Maintenance Code are caused to run and create Event Messages. These Event Messages, generated from the Code, are sent along the local area network (LAN) wire from the Control to the Management Unit. The Management Unit copies the messages from the Code to its storage disk and allows a connected terminal to display them.

Defendants' business is made up in large part of servicing the library systems plaintiff has sold. To do that work effectively and efficiently, they, too, needed a diagnostic tool, and they chose to piggyback on plaintiff's Maintenance Code. Defendants have done so by circumventing the GetKey to gain access to the Maintenance Code and then resetting the maintenance level. They thus stealthily obtain plaintiff's Event Messages, which they transmit to their own computers in Tucson, Arizona. From that data, defendants' service personnel learn what repair functions need to be performed.

To circumvent the GetKey, defendants have used two methods. Until March 2003, defendants used their Library Event Manager (" LEM") device, a computer they attached to the LAN wires that connect to plaintiff's Control and Management Units. A program called "reverse.exe" allowed defendants to defeat the security of the GetKey, albeit through the

sometimes very lengthy process of testing different password combinations until the code was cracked. They would then use the GetKey to set a maintenance level above 0, usually 9, and the system proceeded as designed. After March 2003, defendants used "ELEM," software and a specially designed computer that worked similarly to the LEM, except that it did not use the reverse.exe program. Instead, defendant's ELEM incorporated a forged file identical to one that in the normal course of events would be created by the Control Unit and that tricks the Control Unit to reset the maintenance level at 6, at which level the trickery is not detectable by plaintiff. With both methods, the entire Maintenance Code is perforce copied, and both produced the same results as the GetKey – creation and transmission of the Event Messages.

Plaintiff is likely to succeed on the merits of all three of the claims asserted in support of the motion for a preliminary injunction.

To prove its claim of copyright infringement, plaintiff has to show that 1) it owns a valid copyright in the contested material and 2) defendants copied the protected work. Concrete Machinery, 843 F.2d at 605. Defendants do not dispute that a computer program such as plaintiff's Maintenance Code may be protected by copyright. Rather, they deny that the Event Messages generated by the Maintenance Code are protected, and they vehemently defend any copying of the Maintenance Code as sanctioned by 17 U.S.C. §§ 117(a) and (c) and authorized by plaintiff's license agreements with its customers. Defendants also contest the validity of plaintiff's copyrights.

Infringement first. I find as a matter of fact that defendants copy to RAM the entire Maintenance Code when they use their LEM or ELEM mechanisms for the express

purpose of circumventing plaintiff's GetKey and resetting the Maintenance Level. Such copying infringes plaintiff's copyrights, MAI Systems Corp. v. Peak Computer, Inc. 991 F 2d. 511, 519 (9th Cir. 1993), cert. dismissed, 510 U.S. 1033 (1994), and, contrary to their assertions, defendants are not saved by 17 U.S.C. § 117.[3] That section was passed in 1998 as part of the Digital Millennium Copyright Act to protect computer technicians who risked violating copyright law just by turning on the machines they were to service. Thus, the statute provides that it is not an infringement for the owner or lessee of a machine to authorize the making of a copy of a computer program if the program is copied solely by turning on the machine for the purpose only of maintenance and repair and 1) the copy "is used in no other manner and is destroyed immediately after the maintenance and repair is completed," and 2) any part of the computer program that is not necessary for the machine to be activated is not accessed or used. 17 U.S.C. § 117(c). Defendants copy the Code by turning on the machine; however, they do so 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. Neither the statutory language nor its legislative history is expansive enough to safeguard such use of plaintiff's program. Defendants also fail to destroy the copies they make immediately after completion of repairs. I credit the testimony of plaintiff's expert, Christian B. Hicks, that the copy remains in RAM on an ongoing basis as the system operates with the LEM or ELEM attached.

[3]The claim of infringement by copying Event Messages presents more difficult questions that I need not reach, as plaintiff has proven infringement of its copyrights by other means.

Defendants' contention that plaintiff's licenses to its customers authorize their conduct is unavailing as the licenses simply and explicitly do not encompass the Maintenance Code. That fact further undercuts defendants' §117 argument in that the owners and licensees who have no rights in the Maintenance Code cannot, in any event, authorize its use by defendants.

As for the validity of plaintiff's copyrights, the record shows that plaintiff did erroneously label a derivative work of the 9330 Code as an original version. But the record also shows that it followed the Copyright Office's correction procedures to correct the error, and no evidence has been submitted to show that plaintiff's conduct was knowing, that it harmed defendants or was in any way fraudulent. I am persuaded that all versions of the 9330 Code that had substantial application are registered, and no significant errors were in those applications. The copyrights in suit are valid.

The Digital Millennium Copyright Act provides in 17 U.S.C. § 1201(a) that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title." Plaintiff charges defendants with violating this provision. To sustain its claim, plaintiff has to establish 1) an access control measure that effectively controls access to their work and 2) circumvention of such access control mechanism. Id. The GetKey is unquestionably a qualifying access control measure. It is designed to prevent precisely what defendants achieved, the modification of the Maintenance Level and consequent ability to access the Event Messages. Nor is there any question that defendants bypass the GetKey with their LEM and ELEM devices and that they thereby violate the statute. Defendants' reliance

on §1201(f) is misplaced as that provision only exempts circumvention if it does not constitute infringement, an exemption not applicable in this case.

Plaintiff's final claim is that defendants, by intercepting the Event Messages, misappropriated its trade secret. To make that claim under the Massachusetts statute, plaintiff must show that 1) the Event Messages are trade secrets, 2) it took reasonable steps to protect them, and 3) defendants used improper means to acquire them. Data General Corp. v. Grumman Systems Support Corp., 36 F.3d 1147, 1165 (1st Cir. 1994). A trade secret includes "any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." J.T. Healy & Son, Inc. v. James A. Murphy & Son, Inc., 260 N.E.2d 723, 729 (Mass. 1970).

The Event Messages – the means plaintiff devised to enable it to monitor, maintain and repair the data storage systems it sells – clearly fit within the definition of a trade secret. This is so whether the data alone is considered or whether viewed in combination with the manner of its creation, formulation and transmission.

Plaintiff has unquestionably taken reasonable steps to protect the secrecy of the Event Messages. The GetKey process requires anyone seeking access to jump through not one, but several hoops to get there. The evidence further shows that plaintiff requires its employees to sign confidentiality agreements and that it denies its customers any rights to the Maintenance Code and Event Messages. That there may have been some instances when plaintiff inadvertently allowed a former customer continued access after repairs were completed does not defeat its rights, as the protections it devised and

sustained are reasonable beyond peradventure. The description given above of defendants' methods to gain access surreptitiously to these trade secrets demonstrates the third element, the theft of plaintiff's trade secret.

Plaintiff has shown that defendants' conduct has caused it irreparable harm. First, infringement of copyright and theft of trade secrets require no further proof of harm because harm is presumed. Concrete Machinery, 843 F.2d at 611-12. Second, although I had in earlier stages of these proceedings suggested that money damages were sufficient to make plaintiff whole, the equation has since then changed. The evidence shows that plaintiff's financial losses to date and those projected if the injunction does not issue are far in excess of defendants' ability to pay.

The balance of harm to plaintiff from the denial of the injunction against that to defendant from the grant thereof tilts heavily to plaintiff given its financial losses and damage to its customer relations from defendants' deliberate and calculated misconduct and theft. Lastly, the policy providing for and favoring protection of intellectual property also suggests that the public interest is best served when infringement of rights to and misappropriation of intellectual property are restrained. Id. at 612.

Defendants have interposed antitrust defenses that, they argue, bar the issuance of an injunction. They accuse plaintiff of illegal tying arrangements: Maintenance Code to maintenance service contracts. These allegations appear to have even less merit than the antitrust counterclaims rejected by the Court of Appeals in Data General Corp., 36 F.3d at 1178-81. The record is devoid of any evidence that plaintiff offers to sell to its customers its Maintenance Code if only they will also enter into service contracts. The evidence is all

the other way. Plaintiff does not sell its Maintenance Code separately. Nor does the evidence in the record support defendants' contention that plaintiff has monopoly power in the markets for storage systems and their maintenance. Finally, defendants cannot avoid an injunction against their illegal conduct by alleging violations of antitrust law on plaintiff's part. Id. at 1170 n.43.

The motion for a preliminary injunction is allowed.

_____ /s/ Rya W. Zobel

DATE RYA W. ZOBEL
UNITED STATES DISTRICT JUDGE