Boston University
Journal of Science & Technology Law

Column

Technical Protection Devices and Copyright Law

Neil Smith & Andrew V. Smith

Technical Protection Devices and Copyright Law[†]

Neil Smith[*] & Andrew V. Smith[**]

1. In the digital age, intellectual property moves over the Internet[1] or by other digital transmission simply and inexpensively. Digitized works deserve copyright protection so long as they are original works of authorship.[2] Although copyright law protects the works themselves, enforcing copyrights in the digital environment can be difficult and inefficient because computers enable infringers to make unlimited copies. Technical protection, such as encryption, traditionally used to keep information confidential, can also be used to protect the copyright owner's rights under the Copyright Act.[3] The efficiency of technical protection, however, will depend both on its implementation and on the proscriptions against circumvention. Law prohibiting circumvention of technical protection devices better preserves authors' rights, thereby increasing the incentive to publish digitally.

2. Technical protection devices make data and electronic forms of copyrightable works secure from unauthorized interception, distribution, and copying.[4] Technical protection comes in several forms including encryption,[5] serial

---

 Cite to this column as 3 B.U. J. SCI. & TECH. L. 7 (1997). Pin cite using the appropriate paragraph number. For example, cite the first paragraph of this column as 3 B.U. J. SCI. & TECH. L. 7 para. 1 (1997).

* Neil A. Smith is a partner at Limbach & Limbach, San Francisco. He represented Sega Enterprises, Ltd. in *Sega Enters., Ltd. v. MAPHIA*, 948 F. Supp. 923 (N.D. Cal. 1996).

** Andrew V. Smith, B.S., 1989, State University of New York at Binghamton; M.S., 1991, State University of New York at Binghamton; Ph.D., 1994, Iowa State University; J.D. (anticipated), 1997, Boston University School of Law.

1 The Internet is "a global system of networked computers that allows user-to-user communication and transfer of data files from one machine to any other on the network." JOHN DECEMBER & NEIL RANDALL, THE WORLD WIDE WEB UNLEASHED 6 (2d ed. 1995).

2 Copyrightable works are those that are "original works of authorship, fixed in any tangible medium of expression." 17 U.S.C. § 102(a) (1994).

3 17 U.S.C. §§ 101-1101 (1994).

4 *See* REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS,

copy management systems,[6] steganography,[7] and digital signatures.[8] National attention, however, has been focused on the Clinton Administration's adoption of the Escrowed Encryption Standard ("EES").[9] The EES is particularly controversial because it authorizes law enforcement agencies to decrypt specific messages.[10] Although other encryption standards are available,[11] the Clinton Administration supports the EES standard because it balances the private sector's interest in communications security with the surveillance needs of United States law enforcement.[12]

INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE 230-34 (1995) [hereinafter WHITE PAPER].

5 Encryption is the process of encoding text so that a key must be used to read it. *See* IBM DICTIONARY OF COMPUTING 235 (George McDaniel ed., 1994).

6 Serial copy management systems allow first-generation copies, but prevent the making of perfect digital copies from first-generation copies. *See* Pamela Samuelson, *Regulation of Technologies to Protect Copyrighted Works*, COMM. ASS'N COMPUTING MACHINERY, July 1996, at 17, 21; *see also* 17 U.S.C. § 1002(a), (c) (1994) (requiring digital audio devices to have serial copy management systems and prohibiting circumvention of such systems).

7 Steganography is a method for encoding "digitized information with attributes that cannot be disassociated from the file." WHITE PAPER, *supra* note 4, at 188-89. A party can embed hidden information that does not interfere with the quality of the audio or visual data but stamps the work with a verifiable "watermark." *Id.* at 189. An example of this technique is modulating noise with the information contained in the message or work and distributing this "subliminal noise" throughout the work. *Id.*

8 Just as handwritten signatures verify personal checks and personal documents, digital signatures authenticate electronic transactions and works. *See id.* at 187. The sender encrypts the message or work with his own unique set of binary digits and private key; the receiver can then decrypt the message or work with a private or public key. *See id.* at 188. Digital signatures identify the author and act as a seal, making it possible to verify whether the contents of the file have been altered. *See id.*

9 *See* Federal Information Processing Standards Publication 185, Escrowed Encryption Standards (EES), 59 Fed. Reg. 5997 (1994).

10 Each EES chip has a cryptographic key broken into two components. *See id.* at 6003. Separate federal agencies escrow each component. S*ee id.* at 6005. Constructing the key necessary to decrypt the data requires the retrieval of the key's components from both escrow agents. *See id.* at 6003. However, law enforcement agencies must have a court order before they can retrieve both escrowed components. *Id.* at 6005.

11 Other encryption standards include Pretty Good Privacy ("PGP") and Rivest-Shamir-Adelman ("RSA"). For more information on these standards, see *Pretty Good Privacy, Inc. Homepage* (visited Mar. 28, 1997) <http://www.pgp.com/> and *RSA Homepage* (visited Mar. 28, 1997) <http://www.rsa.com/>.

12 *See* 59 Fed. Reg. at 5998.

3. Although technical protection devices increase the copyright owner's protection from infringement, they are insufficient without legal support. If the copyright owner uses only technical protection, the owner faces three potential problems.[13] First, copiers can bypass technical protection devices with other technical devices.[14] Second, once the copyright owner authorizes a user to use a protected copy, that copy can be duplicated.[15] Third, users may be hesitant to use technologically protected works.[16] Copyright law may be inadequate to address these concerns.

4. Current copyright law does not impose civil or criminal liability on all those who manufacture, sell, or distribute circumvention devices for direct infringement. Instead, those who *knowingly* manufacture, sell, and distribute technical protection circumvention devices may be liable for contributory copyright infringement.[17] Contributory infringement arises when the defendant has "knowledge of the infringing activity [and] induces, causes or materially contributes to the infringing conduct of another."[18] Contributory infringers are subject to damages under section 504(c)(2) of the Copyright Act.[19] Manufacturers and distributors of circumvention devices may intend for their purchasers to infringe the copyrights of others. Although no court has found copyright liability based solely on the circumvention of a technical protection device, contributory infringement liability has been found where the defendant sold or distributed unauthorized copying devices that had no substantially noninfringing purpose.[20]

5. In *Sega Enterprises, Ltd. v. MAPHIA*, the defendant sold devices used to copy

---

13 *See* Symposium, *Protecting Software and Information on the Internet*, 3 B.U. J. SCI. TECH. L. 2 para. 25 (1997) (comments of Pamela Samuelson).

14 *See id.*

15 *See* Pamela Samuelson, *Will the Copyright Office Be Obsolete in the Twenty-First Century?*, 13 CARDOZO ARTS & ENT. L.J. 55, 58 (1994).

16 *See* Ariel B. Taitz, Note, *Removing Road Blocks Along the Information Superhighway: Facilitating the Dissemination of New Technology by Changing the Law of Contributory Copyright Infringement*, 64 GEO. WASH. L. REV. 133, 164 (1995).

17 *See, e.g.,* Sega Enters., Ltd. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996) (finding a BBS operator who sold game-copying devices liable for contributory copyright infringement).

18 Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

19 17 U.S.C. § 504 (c)(2) (1994) (providing increased statutory damages for willful infringement).

20 *Compare Sega*, 948 F. Supp. at 929, *with* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984)(holding videocassette recorders have substantially noninfringing uses).

Sega video games and encouraged users to upload copies to the defendant's bulletin board system ("BBS").[21] The defendant knew about the infringing copying, uploading, and downloading because the defendant actively solicited the infringing uploads and downloads.[22] Thus, the defendant materially contributed to the infringing conduct of the BBS users.[23] The court awarded damages to Sega and enjoined MAPHIA both from selling the devices and from encouraging uploading and downloading by BBS users.[24]

6. Innocently selling a device may not be the basis for an infringement suit, but courts applying *Sega* could find infringement based on the actual circumvention of technical protection devices. The manufacturer or distributor would be materially contributing to the infringement if the circumvention device has no substantially noninfringing purpose.[25]

7. The Clinton Administration has proposed modifications to the Copyright Act to remedy the difficulty of enforcing rights in digitized works.[26] Congress incorporated the proposed modifications in the NII Copyright Protection Act of 1995.[27] The proposed legislation would have added a new chapter to the Copyright Act to support technical protection.[28] This new chapter would prohibit the importation, manufacture, or distribution of devices that bypass technical protection devices.[29] Civil remedies would include injunctive relief, impoundment of infringing articles, and statutory or actual damages.[30]

8. These proposals are similar to the proscriptions against circumvention in

---

21 948 F. Supp. at 929.

22 *See id.*

23 *See id.*

24 *See id.* at 940-41.

25 *See Sony*, 464 U.S. at 442. *Cf.* 17 U.S.C. § 1008 (1994) (prohibiting causes of action based solely on a consumer's manufacture, importation, distribution, or noncommercial use of a digital audio recording device).

26 *See* WHITE PAPER, *supra* note 4, at 230.

27 S. 1284, 104th Cong. (1995); H.R. 2441, 104th Cong. (1995).

28 The proposed chapter would be codified at 17 U.S.C. §§ 1201-1204.

29 *See* S. 1284 § 4; H.R. 2441 § 4.

30 *See id.* Criminal penalties are not available for bypassing a technical protection device under this proposal. *See id.* Criminal penalties are available, however, for giving false copyright management information. *See id.*

the Digital Audio Recording Act.[31] Unlike the NII proposal, the Digital Audio Recording Act actually requires the incorporation of a mandatory technical protection device, or a serial copy management system, in all digital audio recording or interface devices.[32] The Act's civil penalties include injunctive relief, statutory or actual damages, and the impoundment and destruction of violating devices.[33]

9. Compulsory technical protection would provide greater security to copyright owners and would induce them to publish digitally. The purpose of the Copyright Act is to promote the "Progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[34] Giving authors exclusive rights to their works induces them to create and disclose their works.[35] For those authors who do not have the resources to enforce their copyrights, mandatory technical protection would allow them to enforce their copyrights by controlling and discouraging unauthorized copying.[36] Authors who want to renounce their copyrights, or who choose to allow free copying, could presumably use modified copyright management information to provide notice that copying is acceptable.

10. Despite its benefits, however, compulsory technical protection may not be the least restrictive means of promoting the purpose of the Copyright Act. Compulsory protection on all digital documents may completely prohibit access to some public domain works.[37] In addition, compulsory technical protection could restrict even fair uses of copyrighted digital works.[38] Therefore, compulsory technical protection may be contrary to the purpose of copyright law and may restrict both the progress of science and the writings of authors.

---

31 Audio Home Recording Act of 1992, Pub. L. No. 102-563, 106 Stat. 4237, 4240 (codified at 17 U.S.C. § 1002(c) (1994)).

32 17 U.S.C. § 1002(a) (1994).

33 § 1009 (1994).

34 U.S. CONST. art. I, § 8, cl. 8.

35 One object of copyright law is to provide incentives to create and disclose works by providing property rights. *See* 1 PAUL GOLDSTEIN, COPYRIGHT § 1.1 (1989); 1 NEIL BOORSTYN, BOORSTYN ON COPYRIGHT § 1.03 (1996).

36 *See* Nicholas E. Sciorra, *Self-Help and Contributory Infringement: The Law and Legal Thought Behind a Little Black Box*, 11 CARDOZO ARTS & ENT. L.J. 905, 957 (1993).

37 For example, digitized versions of Shakespeare's works might be encoded to prevent copying.

38 The Copyright Act allows for the fair use of a copyrighted work. 17 U.S.C. § 107 (1994). Whether a specific instance of copying is fair use, however, is a fact-specific judicial inquiry that involves weighing several factors. *See id.*

11. Despite these concerns, Congress may move to adopt compulsory technical protection for digital works. The ease and low cost of making identical copies and distributing them over the Internet may completely erode the value of copyright in digital works,[39] thus inciting an outcry in the digital community. If authors are discouraged from publishing digital works, Congress may be compelled to act.

12. Furthermore, the law will not efficiently protect authors' property rights until countries achieve global harmonization both in technical protection device availability and in the laws prohibiting circumvention.[40] Despite strong opposition from the software community,[41] the Clinton Administration has sought to maintain strict controls on the export of encryption technology.[42] In addition Congress has failed to act on a recent proposal that would have eased export restrictions on encryption technology.[43] Although the United States strictly controls the export of encryption technology, strong encryption technology is available domestically and from international suppliers in foreign countries.[44]

13. Most countries probably use encryption and other technical protection devices for national security. Many countries, however, may not be interested in prohibiting the manufacture or distribution of technical protection circumvention devices for several reasons. First, countries that have strong encryption may want to

---

39 *See* Emery Simon, *Innovation and Intellectual Property Protection: The Software Industry Perspective*, COLUM. J. WORLD BUS., Spring 1996, at 30, 33-34 (discussing ease of access and duplication of intellectual property in digital form).

40 *See* Tara Kalagher Giunta & Lily H. Shang, *Ownership of Information in a Global Economy*, 27 GEO. WASH. J. INT'L L. & ECON. 327, 328 (1993).

41 Representatives from several software and encryption companies testified in support of easing encryption export restrictions. *See, e.g., S. 1726, Promotion of Commerce Online in the Digital Era Act of 1996, or "Pro-Code" Act: Hearing on S. 1726 Before the Subcomm. On Science, Tech. & Space of the Senate Commerce Comm.,* 104th Cong. 243-44 (1996) (testimony of Dr. Aharon Friedman, founder of Digital Secured Network Technology) (noting that strict regulation of encryption technology hinders United States companies competing internationally); *id. at* 37 (testimony of Michael Zisman, Chief Executive Officer of Lotus Development Corp.) (promoting export relaxation for non-key escrow encryption products) [hereinafter *Zisman Testimony*].

42 Defense articles and services included on the United States Munitions List may not be exported. *See* Arms Export Control Act, 22 U.S.C. § 2778(a)(1) (1994). The government requires a license to export encryption technology and only grants export licenses for encryption technology up to 56 bits. *See* 15 C.F.R. § 799.1(a) (1996); *cf.* Hiawatha Bray, *Digital, 3 Firms Get Ok to Export Encryption Software*, BOSTON GLOBE, Feb. 4, 1997, at C3 (noting that three companies recently won permission to export 56-bit encryption software).

43 Promotion of Commerce On-line in the Digital Era Act of 1996, S. 1726, 104th Cong. (1996); Promotion of Commerce On-line in the Digital Era Act of 1997, S. 377, 105th Cong. (1997).

44 *See Zisman Testimony*, *supra* note 41, at 38.

maintain circumvention devices for domestic law enforcement and international intelligence gathering.[45] Second, countries with relaxed intellectual property laws may want their citizens to have free access to intellectual property created abroad, such as music, software, and movies.[46] Third, once technical protection devices are common, countries with relaxed intellectual property laws might encourage the manufacturing and mandatory use of circumvention devices to spur economic growth.[47]

14. This disparity in international standards may result in piracy of intellectual property rights by international infringers.[48] In response to this threat, the World Intellectual Property Organization recently considered a treaty that would have required countries to adopt anticircumvention provisions.[49] This provision was similar to the proposed NII Copyright Protection Act of 1995.[50]

15. Although United States copyright law can adequately complement technical protection, recent United States proposals mandating technical protection devices could defeat the purpose of the Copyright Act and inhibit digital publication. In addition, although United States law may be sufficient to support technical protection devices under a contributory infringement analysis, United States authors will not be adequately protected until there is harmonization in international circumvention policies.

---

45 One reason the Clinton Administration supports key escrow programs is that they allow the United States to conduct law enforcement without circumventing technical protection. *See* Federal Information Standards Publication 185, Escrowed Encryption Standards (EES), 59 Fed. Reg. 5997, 6005 (1994).

46 *See* Giunta, *supra* note 40, at 330-31.

47 *See id.* at 328-31.

48 *See id.* at 331.

49 *Draft Treaty on Certain Questions Concerning the Protection of Literary and Artistic Works*, WIPO Doc. CRNR/DC/4 (Aug. 30, 1996) (including a mandatory anticircumvention of technical protection devices provision in article 13). The final Copyright Treaty did not include a mandatory anticircumvention provision but required signatories to "provide adequate legal protection and effective legal remedies" against circumvention devices. WIPO Copyright Treaty, Dec. 20, 1996, 36 I.L.M. 65, 71 (1997) (art. 11).

50 S. 1284, 104th Cong. § 4 (1995); H.R. 2441, 104th Cong. § 4 (1995); *see also* Ron Reiling, *Intellectual Property Regimes for the Technical Age: Policies of the United States, the European Union, and the World Intellectual Property Organization,* 3 B.U. J. SCI. & TECH. L. 9 (1997) (comparing various proposals to revise current intellectual property laws).