Texas Wesleyan Law Review

Volume 8 | Issue 3 Article 10

7-1-2002

The Anti-Circumvention Provision of The Digital Millennium Copyright Act

Herbert J. Hammond

Heather C. Brunelli

Jocelyn E. Dabeau

Luke A. Walker

Thomas Yoo

Recommended Citation
Herbert J. Hammond, Heather C. Brunelli, Jocelyn E. Dabeau, Luke A. Walker & Thomas Yoo, *The Anti-Circumvention Provision of The Digital Millennium Copyright Act*, 8 Tex. Wesleyan L. Rev. 593 (2002).
Available at: https://doi.org/10.37419/TWLR.V8.I3.9

THE ANTI-CIRCUMVENTION PROVISION OF THE DIGITAL MILLENNIUM COPYRIGHT ACT

Herbert J. Hammond†
Heather C. Brunelli††
Jocelyn R. Dabeau†††
Luke A. Walker††††
Thomas Yoo†††††

I. INTRODUCTION

For evidence of the growing digital economy, one does not need to look far. According to a report released by the U.S. Department of Commerce in 1998,[1] sales of computer hardware, software, and networking products and services are growing at unprecedented rates. The information-technology sector, in 1998, accounted for an

† Partner, Intellectual Property, Thompson & Knight LLP, 1700 Pacific Avenue, Suite 3300, Dallas, Texas, 75201; J.D., New York University School of Law, New York, New York; B.S., University of New Mexico, Albuquerque, New Mexico.

†† Associate, Intellectual Property, Thompson & Knight LLP, 1700 Pacific Avenue, Suite 3300, Dallas, Texas, 75201; J.D., Boston College Law School, Newton, Massachusetts; B.A., Wellesley College, Wellesley, Massachusetts.

††† Associate, Intellectual Property, Thompson & Knight LLP, 1700 Pacific Avenue, Suite 3300, Dallas, Texas, 75201; J.D., Harvard Law School, Cambridge, Massachusetts; B.A., University of Texas, Austin.

†††† Associate, Intellectual Property, Thompson & Knight LLP, 1700 Pacific Avenue, Suite 3300, Dallas, Texas, 75201; J.D., University of California at Berkeley School of Law, Boalt Hall, Berkeley California; B.A., Phillips University, Enid, Oklahoma.

††††† Associate, Intellectual Property, Thompson & Knight LLP, 1700 Pacific Avenue, Suite 3300, Dallas, Texas, 75201; J.D., University of Texas School of Law, Austin, Texas; B.S., University of Texas, Austin, Texas.

1. *See* SECRETARIAT ON ELEC. COMMERCE, U.S. DEP'T OF COMMERCE, THE EMERGING DIGITAL ECONOMY (1998).

DOI: https://doi.org/10.37419/TWLR.V8.I3.9

estimated 8.2 percent of the U.S. gross domestic product and for more than 25 percent of the country's real economic growth.[2] Today, electronic commerce and the Internet have become an integral part of our daily life. In 1998, the Clinton Administration, seeking to provide both a legal framework for copyright protection in the emerging digital economy and to comply with new international treaties, sponsored the Digital Millennium Copyright Act (DMCA), which includes, among other provisions, a ban on circumventing technological access-control measures in digital works.

The DMCA's ban on circumvention technology, however, has been the subject of some dispute. In the "arms race" between encryption and decryption technologies, the anti-circumvention provision seems to have recently won out. The anti-circumvention provision also appears to have altered the contours of copyright law and to have disturbed the balance between protecting the rights of authors and promoting the advancement and flow of information. This Article begins with a brief history of the Digital Millennium Copyright Act and its anti-circumvention provision. It then describes the features of the anti-circumvention provision, its exceptions, and the remedies provided by the Act. Finally, it reviews three recent cases that raise important issues that, when ultimately resolved, may permanently affect copyright law.

II. A Brief History of the DMCA

In December 1996, the United States signed and ratified the World Intellectual Property Organization (WIPO) Copyright Treaty.[3] This treaty provided several international norms for extending copyright protection to digital works. One of these norms required that signatory countries provide "adequate legal protection and effective legal remedies"[4] against the circumvention of technical measures used by copyright owners to protect copyrighted digital works from infringement.

To comply with the WIPO Copyright Treaty's mandates, the Clinton Administration proposed the Digital Millennium Copyright Act,

2. *Id.* at 1–7.

3. WIPO Copyright Treaty, Dec. 2, 1996, WIPO Doc. CRNR/DC/94 *available at* http://www.wipo.int/eng/diplconf/distrib/94dc.htm; Treaties and Contracting Parties: Intellectual Property Protection Treaties, WIPO Copyright Treaty: Contracting Parties (April 15, 2002), *available at* http://www.wipo.int/treaties/ip/wct/index.html. The United States also entered into another WIPO treaty in 1996, WIPO Performances and Phonograms Treaty, Dec. 2, 1996; WIPO Doc. CRNR/DC/95, *available at* http://www.wipo.int/eng/diplconf/distrib/95dc.htm. In addition, some of the provisions and remedies discussed below may apply both to the anti-circumvention provision as well as other provisions of the DMCA, such as § 1202, which addresses itself to the misuse of copyright-management information. The scope of this paper, however, is limited to the anti-circumvention provision.

4. WIPO Copyright Treaty, *supra* note 3, at art. 11.

which, among other things, included a strong and sweeping anti-circumvention provision.[5] As one might expect, the proposed legislation fostered intense lobbying by interested parties on both sides of the issue. On one side of the debate, copyright owners stressed the need for strong measures to protect their copyrights in digital environments in which illegal copies can be transmitted effortlessly and perfectly to millions almost instantaneously. At the other end of the spectrum, libraries, academia, and consumer-rights groups decried the proposed anti-circumvention provision as too sweeping, and criticized it for turning back the clock to prevent uses of electronic information that were legal under the existing Copyright Act.

The original anti-circumvention provision proposed by the Clinton Administration was simple and unyielding: it banned all circumvention activity except for law-enforcement or intelligence purposes. Congressman Bliley of the Commerce Committee expressed concern that this provision, "[i]f left unqualified, . . . could well prove to be the legal foundation for a society in which information becomes available only on a 'pay-per-use' basis;"[6] ultimately, the major information-technology firms convinced Congress that there were legitimate reasons to circumvent technical-protection systems, such as encryption research and computer-security testing.[7] Congress responded to these legitimate reasons for circumvention not by narrowing the scope of the proposed anti-circumvention provision, but by creating specific exceptions. Clinton's administration officials admitted in Congressional testimony that the proposed anti-circumvention provision, in fact, went beyond what was necessary to comply with the WIPO Copyright Treaty, but they defended the legislation as a means to convince other countries to adopt similarly strong standards.[8]

Despite Congressman Bliley's concerns and despite the lobbying efforts of the libraries, academia, and consumer advocates, the anti-circumvention provision may have come close to creating the pay-per-access distribution model feared by some, at least in the digital do-

5. In addition to the anti-circumvention provision, the passage of the DMCA has established two other statutory changes to copyright law in the digital environment. First, it created a safe harbor for online service providers (typically ISPs) against copyright infringement liability for messages posted to the providers' systems. Second, it created a cause of action for misuse or destruction of "copyright management information." The anti-circumvention provision though, has been, by far, the most controversial change to copyright law.

6. 144 CONG. REC. H7094 (daily ed. Aug. 4, 1998) (statement of Rep. Bliley).

7. For a more specific discussion of the lobbying activities and legislative history behind the anti-circumvention provision, see Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999).

8. The European Union Council of Ministers adopted the Directive on Copyright in 2001, which contained a parallel anti-circumvention provision to the DMCA. The EU anti-circumvention provision is equally strict, providing only specific exceptions to a general and broad ban on circumvention acts.

main. Critics continue to argue that the anti-circumvention provision has created a whole new level of copyright protection for digital works, which would not be available under traditional copyright law, by banning the instrumentality rather than the act of copying. If nothing else, the end result of the DMCA's passage has been to create a very broad and stringent provision with few, very narrow exceptions. The influence that the anti-circumvention provision will have on copyright law, however, has yet to be felt because the most prominent challenges so far—fair use, First Amendment, contributory infringement, and criminal liability—have yet to be fully resolved by the courts. The *Remierdes*, *ElcomSoft*, and *Felton* cases, discussed below, illustrate how the courts are trying to flesh out the content of this unprecedented fixture of copyright law.

III. The Substantive Provisions of the DMCA

The DMCA prohibits (1) acts of circumvention; (2) devices that circumvent access-control measures; and (3) devices that circumvent copyright-protection control measures.[9] The Act's anti-circumvention provision can be violated by simply bypassing security measures without actually committing acts of infringement. Some proponents of the DMCA have analogized the violation of the DMCA's anti-circumvention provisions to "breaking into a library to read books."

The first of these sections targets circumvention itself. Section 1201(a)(1)(A) of the DMCA bans the act of circumventing "a technological measure that effectively controls access to a work protected under this title"[10] and by "this title," the provision is referring to the 1976 Copyright Act codified in Title 17 of the U.S. Code. This provision prevents the circumvention of access-control measures that "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[11] Circumvention, under the DMCA, means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[12] Seven specific exceptions to the DMCA's ban on the act of circumvention will be dealt with in Section IV below.

Next, the DMCA contains two different "anti-device" or "anti-trafficking" provisions: §§ 1201(a)(2) and 1201(b)(1). The anti-device provisions outlaw the manufacture or distribution of any technological device that enables users to circumvent control measures imposed by copyright owners. In both cases, § 1201 states that "[no] person shall

9. Other aspects of the DMCA, such as the general protection for Internet service providers from liability, are outside the scope of this Article.

10. 17 U.S.C. § 1201(a)(1)(A) (2000).

11. *Id.* § 1201(a)(3)(B).

12. *Id.* § 1201(a)(3)(A).

manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof"[13] if it (1) "is primarily designed or produced for the purpose of circumventing;"[14] (2) "has only a limited commercially significant purpose or use other than to circumvent;"[15] or (3) "is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing."[16] The anti-device provisions are subject to a more limited array of exceptions than § 1201(a)(1)'s ban on the act of circumvention.

The second major prohibition of the DMCA, found in § 1201(a)(2), seeks to prevent circumvention of access controls. An access control is "a technological measure that effectively controls access to a [copyrighted] work."[17] The legislative history of this section indicates that Congress modeled this provision after existing laws banning "black boxes," which function to descramble cable-television and satellite-cable services.[18]

The third major prohibition, found in § 1201(b)(1), forbids circumvention of copy controls—measures employed by copyright owners to prevent unauthorized duplication and other forms of copyright-infringing conduct. Section 1201(b)(1) prohibits the circumvention of the "protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof."[19]

IV. THE SEVEN EXCEPTIONS TO THE ANTI-CIRCUMVENTION PROVISION

As expected, the proposed anti-circumvention provision was met with both unbridled enthusiasm from the entertainment industry, particularly from Hollywood and the music industry, and naysaying by academics and civil liberties groups, who argued that the ban detrimentally affected legitimate circumvention activities. In response, Congress sought a compromise that would keep the strong language of the statute but assuage the fears of some of the provision's opponents. This sought-after compromise ultimately led to a set of specific exceptions.[20]

13. *Id.* § 1201(a)(2), (b)(1).
14. *Id.* § 1201(a)(2)(A), (b)(1)(A).
15. *Id.* § 1201(a)(2)(B), (b)(1)(B).
16. *Id.* § 1201(a)(2)(C), (b)(1)(C).
17. *Id.* § 1201(a)(1)(A).
18. H.R. REP. NO. 105–551, pt. 2, at 38 n.2 (1998).
19. 17 U.S.C. § 1201(b)(1)(A)–(C).
20. In addition to the seven enumerated exceptions, Congress placed a two-year moratorium on the enforcement of the actual anti-circumvention provision (as opposed to the "trafficking" provision), which expired in 2001. During the moratorium, Congress gave to the Librarian of Congress (with recommendations from the Register of Copyrights and the Assistant Secretary of Commerce for Communications and In-

- *The government activities exception.*[21] The most comprehensive exception applies to the entire anti-circumvention provision, exempting all legitimate law-enforcement, intelligence, and other governmental activities.
- *The nonprofit library, archive, and educational institution exception.*[22] Nonprofit libraries, archives, and educational institutions are permitted to circumvent access-control measures solely for the purpose of making a good faith determination regarding whether they wish to obtain authorized access to a protected work.
- *The reverse-engineering exception.*[23] This exception permits circumvention— and the development of technological means for such circumvention—by a person who has lawfully obtained a copy of a computer program for the sole purpose of identifying and analyzing elements of the program necessary to achieve interoperability with other programs, to the extent that such acts are permitted under copyright law.
- *The encryption-research exception.*[24] Encryption researchers are permitted to circumvent access-control measures to identify flaws and vulnerabilities in encryption technologies.
- *The protection-of-minors exception.*[25] This exception allows a court applying the prohibition to a component or part to consider the necessity for its incorporation in technology that prevents access of minors to material on the Internet.
- *The personal-privacy exception.*[26] This exception permits circumvention when the technological measure, or the work it protects, is capable of collecting or disseminating personally identifying information about the online activities of a natural person.
- *The security-testing exception.*[27] This exception permits circumvention of access-control measures and the development of technological means for such circumvention, for the purpose of testing the security of a computer, computer system or computer network if it is done with the authorization of its owner or operator.

---

formation) the duty to study the potential impact of the anti-circumvention ban on non-infringing uses and to propose additional exceptions as it deemed necessary. After reviewing the issues and arguments presented for additional exceptions, the Librarian of Congress chose to propose only two additional exceptions to those enumerated in the original DMCA. The first additional exception allows parties to circumvent encrypted Internet filtering compilations of restricted sites to comment or criticize the compilations. The second exception allows circumvention of access controls to literary works that have malfunctioned. The next recommendation period is scheduled for 2003.

21. 17 U.S.C. § 1201(e).
22. *Id.* § 1201(d).
23. *Id.* § 1201(f).
24. *Id.* § 1201(g).
25. *Id.* § 1201(h).
26. *Id.* § 1201(i).
27. *Id.* § 1201(j).

Possibly more important than any of these specific exceptions to the anti-circumvention provision is one notable exception that has been excluded—the "other-legitimate purposes exception." Many situations arise where circumvention of an access-control measure may be necessary but not authorized by the anti-circumvention provision's specific exceptions. If a copyright owner suspects that an encrypted work contains infringing material, for example, the copyright owner may be unable to investigate the potential infringement without circumventing the infringer's technical protection system. Even if infringement is later established, the copyright proprietor will have violated the anti-circumvention provision in proving it.[28] The lack of any catchall exception leaves courts with the unenviable task of having to choose between stretching an existing exception to cover circumvention for a legitimate or laudable purpose, broadly interpreting the "defenses"[29] section of the anti-circumvention provision, or reaching an unjust result. As one commentator has noted, instead of forcing the courts to "thrash" around, Congress should have simply included an exception for other legitimate circumvention purposes.[30] Unfortunately, this did not occur, creating some practical problems. As evidenced in the *Felton* case, discussed below, the absence of an "other-legitimate purposes exception" creates unnecessary fear and legal uncertainty for clearly legitimate uses of circumvention technology.

V. Civil Remedies and Criminal Penalties

Any person injured by anti-circumvention may bring a civil action in federal court.[31] The civil remedies for violation of the anti-circumvention provision parallel those for copyright infringement, including actual or statutory damages and injunctive relief.[32] Like copyright infringement, actual damages for acts of anti-circumvention may include any actual damages suffered by the injured party as a result of the violation as well as any profits of the violator attributable to the violation that are not taken into account in computing the actual damages.[33] The court can award statutory damages ranging from $200 to $2500 per act of circumvention, and the court has discretion to reduce

28. This example and many others are provided by Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Tech. L.J. 519, 543–45 (1999).

29. 17 U.S.C. § 1201(c)(1) (providing that, "[n]othing in this section shall affect rights, remedies, limitations or defenses to copyright infringement, including fair use").

30. Samuelson, *supra* note 28, at 545.

31. *Id.* § 1203(a).

32. *See id.* § 1203(b)–(c).

33. *Compare id.* § 1203(c)(2), *with* § 504(b).

the damages in cases involving unintentional or innocent violations.[34] Just as these damages may be reduced at the court's discretion for innocent violations, the court, in the case of repeated violations, may also increase the damages up to triple the amount that would otherwise be awarded.[35]

In addition to awarding monetary damages, the same arsenal of remedies available for copyright infringement are available for violations of the anti-circumvention provision. The court has discretion to impound devices believed to be involved in the asserted violation,[36] to grant temporary and permanent injunctions (provided the injunction does not impose a prior restraint on free speech or the freedom of the press in violation of the First Amendment),[37] to allow the recovery of costs (except to or against the United States), to award reasonable attorneys' fees to the prevailing party,[38] and finally, upon final judgment, to order the destruction or modification of any devices that violate the anti-circumvention provision.[39] Although the anti-circumvention provision contains no statute of limitations per se, it presumably is subject to the limitations provision in § 507(b) that applies to "provisions of this title."[40]

As severe as the provision's civil penalties are (statutory damages may be as high as $2500 per act), it is the criminal penalties that have made the anti-circumvention provision truly controversial. Under § 1204's criminal provisions, anyone who *willfully* violates the anti-circumvention provision for "purposes of commercial advantage or private financial gain" can be fined up to $500,000 or imprisoned for up to five years, or both, for a first offense.[41] The penalties are increased to up to a $1,000,000 fine and up to 10 years' imprisonment for subsequent offenses. Again, the criminal provision essentially tracks those in § 506 of the Copyright Act for willful copyright infringement. The same five-year statute of limitations applicable to copyright infringement,[42] applies to criminal acts; nonprofit libraries, archives, and educational institutions, however, are entirely exempted

34. *Id.* § 1203(c)(5)(A). The violator has the burden of proving that he or she was neither aware nor had reason to believe that the act constituted a violation. *Id.*

35. *Id.* § 1203(c)(4). To prove repeated violations, the injured party must establish that a person has violated the anti-circumvention provision (or the copyright management information statute, § 1202) within 3 years after a final judgment was entered against that person for another violation. *Id.*

36. *Id.* § 1203(b)(2).

37. *Id.* § 1203(b)(1).

38. *Id.* § 1203(b)(4)–(5).

39. *Id.* § 1203(b)(6).

40. *Id.* § 507(b) (providing that "[n]o civil action shall be maintained under the provisions of this title unless it is commenced within three years after the claim accrued").

41. *Id.* § 1204(a).

42. *Id.* §§ 506(a)(2), 507(a).

from criminal but not civil liability.[43] The imposition of criminal penalties, as discussed below, is particularly unprecedented in our copyright-law jurisprudence because criminal conviction for violation of the anti-circumvention provision does not require proof that any copyright infringement occurred. Again, to extend the analogy to the criminal law, it is sufficient to "break into the library to read the book."

VI. BEGINNING THE DEBATE: *UNIVERSAL CITY STUDIOS, INC. V. REMIERDES*

Not surprisingly, the major motion-picture studios in Hollywood (who were probably among the biggest backers of the WIPO amendments and the DMCA's implementation of the WIPO amendments that followed) were the first to try to take advantage of the DMCA's anti-circumvention provision. The impetus for the *Remierdes* case was a concern on the part of studios and producers over illegal copying of their motion pictures encoded onto DVDs[44] with the Content Scramble System or CSS encryption technology.[45] A program called DeCSS, which can be used to circumvent CSS and disable the encryption mechanism contained in DVDs that prevents unauthorized copying, was originally developed by a Norwegian teenager and later refined by open-source programmers in communities on the Internet around the world. The DeCSS program was published on websites internationally: anyone who wanted a copy of the program could simply download it from one of these websites and use it to make unauthorized copies of movies encrypted on DVDs.

The eight major motion-picture studios, producers, and distributors of the majority of the motion pictures on DVDs filed suit in the Southern District of New York to enjoin these website operators from posting DeCSS on their sites.[46] Judge Kaplan held that the defendants' posting of the DeCSS program on their websites, as well as their linking to other websites containing the DeCSS program, violated the DMCA's anti-circumvention provisions, and he issued a permanent injunction prohibiting them from either posting DeCSS on their web-

43. *Id.* § 1204(b)–(c). This exemption from criminal liability, however, does not apply to repeated violations. *See id.* § 1201(d)(3)(B). Moreover, nonprofit libraries, archives, and educational institutions are entitled to complete remission of all civil damages awarded only in instances of innocent violations. *Id.* § 1203(c)(5)(B)(ii).

44. A DVD, or digital versatile disc, is an optical media storage device that can be used to record and play a movie in digital form, much as a compact disc ("CD") can be used to record and play songs contained in digital form. DVDs are encrypted by their producers with the Content Scramble System, or CSS.

45. CSS is an encryption technology designed to prevent unauthorized copying of the content of the discs. CSS should prevent the owner (or holder) of a DVD from copying the DVD and sharing copies of its digital contents with unauthorized third parties.

46. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 303 (S.D.N.Y. 2000).

sites or from knowingly linking to any other websites containing DeCSS.[47]

Corley, one of the defendants who had unsuccessfully challenged the constitutionality of the anti-circumvention provision in the district court, appealed, arguing that: (1) the DMCA oversteps limits in the Copyright Clause on duration of copyright protection; (2) the DMCA as applied to his dissemination of DeCSS violated the First Amendment because computer code is "speech" and the DMCA does not meet the exacting standards required to regulate "speech;" and (3) the DMCA violates the First Amendment and the Copyright Clause by unduly obstructing the "fair use" of copyrighted material. He was assisted in his appeal by a group of law professors and civil liberties groups, some of whom filed amicus briefs supporting his position.

The Second Circuit Court of Appeals affirmed.[48] Writing for the court, Judge Newman held that, while a computer program like DeCSS may be "speech" for First Amendment purposes, Congress's goal in adopting the DMCA's anti-circumvention and anti-trafficking provisions was content-neutral, and the restriction was aimed at the computer code's *function* rather than any particular expression. Thus, the court reasoned that the defendants' inability to continue posting or linking to DeCSS in violation of the DMCA was not an impermissible burden on the exercise of their First Amendment rights.[49] Further, the court found that the anti-circumvention and anti-trafficking provisions did not impermissibly restrict "fair use" because the defendants did not claim to be making any fair use of copyrighted materials, but were merely providing others with the opportunity to use a program designed to thwart copyright owners' efforts to protect their copyrighted works in violation of the DMCA.[50] Because the defendants had presented no evidence that those who wanted to access the copyrighted materials for purposes of education or commentary would be prevented from gaining it from copyright owners, the court found it unnecessary to determine whether there was a constitutional right to fair use in this case.[51]

VII. CRIMINAL VIOLATIONS: *U.S. v. ELCOMSOFT AND DMITRY SKLYAROV*

The first criminal prosecution under the anti-circumvention provision was brought against software developers in the Northern District of California. The indictment charged a Russian computer programmer and his employer, ElcomSoft, with violations of §§ 1201(b)(1)(A)

47. *Id.* at 324–25, 346.
48. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 460 (2d Cir. 2001).
49. *See id.* at 442.
50. *See id.* at 459.
51. *See id.* at 458–59.

and 1201(b)(1)(C) based on ElcomSoft's distribution of a program called Advanced eBook Processor or "AEBPR over the Internet."

The background of the case is as follows. Adobe Systems, Inc. produces a product called Adobe Acrobat eBook Reader that provides the technology that allows purchasers to read electronic books (eBooks) in digital form on computers.[52] Adobe's eBook software allows the publisher of an eBook to authorize or limit a purchaser's ability to copy, distribute, print, or have the text of an eBook audibly read by the computer.[53] The software prevents the purchaser of an eBook from printing a partial or entire copy of the book and prevents the purchaser from transporting the eBook file from one computer to another.

Dmitry Sklyarov is a twenty-seven-year-old computer programmer and Ph.D. student researching cryptanalysis at Moscow University. He is employed by the Russian company, ElcomSoft Co., Ltd., which develops various computer security products. ElcomSoft specializes in password recovery software and computer forensic tools.[54] Sklyarov worked on algorithms for AEBPR for ElcomSoft. The AEBPR program allows the owner of an eBook to remove the usage restrictions and view his or her eBook in any Portable Document Format (PDF) viewer. The program essentially allows the eBook to be printed, transferred to another computer, or copied to a disk.

Adobe Systems, Inc. contacted the FBI last June about the AEBPR product. Following an FBI investigation, Sklyarov was arrested in Las Vegas on July 16, 2001, after attending and speaking at the DEF CON conference.[55] The Electronic Frontier Foundation and other activist groups protested his arrest and jailing. Adobe withdrew its support for the criminal complaint after a public outcry, and Sklyarov was released on $50,000 bond on August 6. On August 28, 2001, Sklyarov and ElcomSoft were indicted for violations of the anti-circumvention provisions of the DMCA. On December 13, Sklyarov entered into an agreement with the government in which he admitted to the conduct charged in the indictment and agreed to cooperate with the United States in the ongoing prosecution of ElcomSoft. Under the agreement, he is required to appear at trial and testify for the United States. The United States has agreed to defer prosecution of Sklyarov until

52. Defendant's Motion to Dismiss Indictment for Violation of Due Process at 6, United States v. Elcom Ltd., No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002).

53. U.S. Attorney's Indictment, *Elcom*, No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002).

54. Defendant's Motion to Dismiss Indictment for Violation of Due Process at 3, United States v. Elcom Ltd., No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002).

55. The DEF CON conference is an annual technical conference attended by professional and amateur security experts, cryptographers, computer programmers, and self-styled hackers.

the conclusion of the case against ElcomSoft, or for a year, whichever is longer, and Sklyarov has been permitted to return to Moscow. If Sklyarov completes his obligations, the United States will dismiss the charges pending against him.

The indictment against ElcomSoft and Dmitry Sklyarov contains five counts. The first count is under 18 U.S.C. § 371 for "conspiracy to traffic in technology primarily designed to circumvent, and marketed for use in circumventing, technology that protects a right of a copyright owner."[56] The remaining counts are based upon the anti-circumvention provision itself. The second and third counts charge the defendants with trafficking in technology primarily designed to circumvent technology that protects a right of a copyright owner in violation of § 1201(b)(1)(A).[57] The fourth and fifth counts allege trafficking in technology marketed for use in circumventing technology that protects a right of a copyright owner, in violation of § 1201(b)(1)(C).[58]

Under the indictment, Sklyarov faces a prison term of up to twenty-five years and a fine of up to $2,250,000. ElcomSoft, as a corporate defendant, faces a potential fine of $2,250,000.

---

56. U.S. Attorney's Indictment at 5, *Elcom*, No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002).

57. Count two, based upon violation of 17 U.S.C. § 1201(b)(1)(A) (2000), charges that the defendants:

> did willfully, and for purposes of commercial advantage and private financial gain, offer to the public and traffic in a technology, product, device, component, and part thereof, that was *primarily designed and produced* for the purpose of circumventing protection afforded by a technological measure that effectively protected a right of a copyright owner under Title 17 of the United States Code, in a work and portion thereof, in that the defendants offered the AEBPR program to the public for sale in the Northern District of California.

U.S. Attorney's Indictment at 5, *Elcom*, No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002) (emphasis added). Count three is also based upon violation of 17 U.S.C. § 1201(b)(1)(A) and repeats the language of the second count, only basing the violation on the fact that the defendants allegedly "sold a copy of the AEBPR program to an individual in the Northern District of California." *Id.*

58. Count four is based upon a violation of 17 U.S.C. § 1201(b)(1)(C), that the defendants:

> did willfully and for purposes of commercial advantage and private financial gain, offer to the public and traffic in a technology, product, device, component, and part thereof, that was *marketed* by the defendants and others acting in concert with the defendants' knowledge, for use in circumventing protection afforded by a technological measure that effectively protected a right of a copyright owner under Title 17 of the United States Code, in a work and portion thereof, in that the defendants marketed the AEBPR program in the Northern District of California.

U.S. Attorney's Indictment at 6, *Elcom*, No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002) (emphasis added). Count five is also based upon violation of 17 U.S.C. § 1201(b)(1)(C) and repeats the language of the fourth count, only basing the violation on the fact that the defendants "sold a copy of the AEBPR program in the Northern District of California." *Id.*

Criminal prosecution under the anti-circumvention provisions of the DMCA raises a host of important, yet unanswered issues. Can or should the United States prosecute foreign nationals and foreign corporations for violations of a U.S. law in connection with acts that occurred and were legal in that foreign country? Does the DMCA impermissibly infringe on the First Amendment? Does the DMCA go too far in attempting to protect U.S. copyrights? Should criminal liability be imposed if no copyright infringement is actually facilitated?

ElcomSoft's attorneys have raised the foreign nationals issue by moving to dismiss the indictment for lack of jurisdiction on grounds that § 1201 of the DMCA should not be applied to a foreign corporation for conduct that occurred outside the U.S. or entirely on the Internet because such conduct is outside the territorial jurisdiction of the United States.[59]

AEBPR was developed by ElcomSoft's employees in Russia.[60] Last June, the program was offered for sale on the Internet.[61] In a motion to dismiss the charges based on a lack of jurisdiction, ElcomSoft argued that Congress expressed no intent to give the statute extraterritorial effect and that giving it extraterritorial effect violates due process.[62] ElcomSoft also argued that it had no warning that § 1201 would be applied to its conduct; that it had no intent to engage in any criminal acts by offering its AEBPR program for sale; that it did not develop a plan for sale of the AEBPR program in the United States; and that it did not direct the advertising of the AEBPR program towards the United States or advertise AEBPR in publications distributed or sold in the United States.[63] ElcomSoft has also argued that it has conducted its activities consistent with Russian law, under which development and sale of the AEBPR program would not be illegal.[64] Finally, ElcomSoft has made the point in its motion to dismiss that if the court exercises jurisdiction over ElcomSoft for alleged violations of § 1201, the court would be subjecting ElcomSoft to laws that conflict with the regulations of another sovereign and that doing so would violate international law.[65]

Another intriguing issue raised by the ElcomSoft indictment is whether the DMCA's anti-trafficking provisions violate the First Amendment.[66] In its defense, ElcomSoft argued that the anti-circum-

59. Notice of Motion and Motion to Dismiss Indictment for Lack of Jurisdiction at 1, *Elcom*, No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002).

60. *Id.* at 3.

61. *Id.*

62. *Id.* at 7–8.

63. *Id.* at 10–11.

64. *Id.* at 17–18.

65. *Id.* at 18.

66. Reply Memorandum of Points and Authorities in Support of Motion to Dismiss Based on First Amendment at 1, *Elcom*, No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002).

vention provision is "fundamentally flawed because it targets expression rather than the conduct with which it purports to be concerned." Computer programs, ElcomSoft argues, are a form of expression.[67] ElcomSoft has raised the interesting argument that because computer code is "protected speech" and the DMCA burdens more speech than is necessary to serve the government's interest, the DMCA violates the First Amendment.[68] The district court judge, however, did not agree. The court concluded that intermediate scrutiny rather than strict scrutiny was the appropriate standard to apply.[69] Although the court agrees that computer code was "speech," it applied an intermediate-scrutiny standard and held that "a statute is constitutional as long as it 'promotes a substantial government interest that would be acheived less effectively absent the regulation' and the means chosen do not burden substantially more speech than is necessary to further the government's legitimate interest."[70] The court found that the government's interests in preventing the unauthorized copying of copyrighted works and promoting electronic commerce were both legitimate and substantial.[71] The court went on to determine that the statute was sufficiently tailored to promote these interests:

> targeting the tool sellers is a reasoned, and reasonably tailored, approach to "remedying the evil" targeted by Congress. In addition, because tools that circumvent copyright protection measures for the purpose of allowing fair use can also be used to enable infringement, it is reasonably necessary to ban the sale of all circumvention tools in order to achieve the objectives of preventing widespread copyright infringement and electronic piracy in digital media. Banning the sale of all circumvention tools thus does not substantially burden more speech than is necessary.[72]

In its motion to dismiss, ElcomSoft also claimed that the DMCA is unconstitutionally vague and, therefore, violates the Due Process Clause of the Fifth Amendment.[73] The court again rejected ElcomSoft's arguments. The court found that a statute is not impermissibly vague if all tools that are primarily designed or produced for the purpose of circumventing the protections afforded by technology are

67. *Id.*

68. *Id.* at 3.

69. Order Denying Defendant's Motion to Dismiss the Indictment on Constitutional Grounds at 16, United States v. Elcom Ltd., No. CR 01-20138 RMW (N.D. Cal. May 8, 2002).

70. *Id.*

71. *Id.* at 17.

72. *Id.* at 20.

73. Reply Memorandum of Points and Authorities in Support of Motion to Dismiss Based on First Amendment at 13, United States v. Elcom Ltd., No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002).

banned.[74] And because the statute does, in fact, ban trafficking in or the marketing of all circumvention devices,[75] the court found that the law allows a person to conform his or her conduct to a comprehensible standard and is thus not unconstitutionally vague.[76]

Finally, Elcomsoft challenged the DMCA by arguing that Congress exceeded its authority in enacting the DMCA and that, as a result, the statute is unconstitutional. The court quickly rejected any implication that Congress did not have the power to enact the DMCA under the Commerce Clause.[77] The court stated:

> To the extent that circumvention devices enable wrongdoers to engage in on-line piracy by unlawfully copying and distributing copyrighted works of authorship, the sale of such devices has a direct effect on suppressing the market for legitimate copies of the works. Accordingly, there is a rational basis for concluding that the regulated activity sufficiently affects interstate commerce to establish that Congress had authority under the Commerce Clause to enact the legislation.[78]

The court, however, found it more difficult to decide whether Congress was precluded from enacting the DMCA by the restraint imposed by the Intellectual Property Clause.[79] Nonetheless, the court found that protecting the exclusive rights granted to copyright owners against unlawful piracy was consistent with the Intellectual Property Clause's grant to Congress of the power to promote the useful arts and sciences,[80] and that the DMCA is not irreconcilably inconsistent with the limitations contained within the Intellectual Property Clause.[81]

Because the DMCA criminalizes the circumvention of just about any electronic security measure, ElcomSoft and others argue the DMCA infringes upon the public's right to access and use non-copyrighted works. If the AEBPR program were used to circumvent anti-copying provisions that prevent, for example, the copying of public-domain works, such anti-circumvention acts would still be illegal under the DMCA. Similarly, if AEBPR or some other anti-circumvention program were used to circumvent measures that prevent owners of eBooks or other electronic files from making an archival copy, or copying an excerpt from an eBook, a good argument could be

74. Order Denying Defendant's Motions to Dismiss the Indictment on Constitutional Grounds at 8, United States v. Elcom Ltd., No. CR 01-20138 RMW (N.D. Cal. May 8, 2002).

75. *Id.* at 11.

76. *Id.*

77. *Id.* at 27–28.

78. *Id.* at 28.

79. *Id.*

80. *Id.* at 30.

81. *Id.* at 31.

made that acts that would otherwise be permitted under the archival[82] or fair-use[83] exceptions of the Copyright Act are effectively precluded by the anti-circumvention provision. In other words, what the right hand of the Copyright Act giveth in the archival-copying and fair-use exceptions in the first chapter of the Copyright Act, the left hand taketh away in the last.

The question of whether criminal sanctions should be available under the anti-circumvention provision in the absence of any infringement, or in circumstances where acts of circumvention do not facilitate infringement, continues to be one of the most controversial aspects of the DMCA. The indictments of ElcomSoft and Sklyarov are a case in point: those indictments are not based on any claim by the government that AEBPR was used to unlock an eBook program as part of a scheme to disseminate illegal copies. In fact, AEBPR only disables access controls on eBooks that are legally purchased by consumers.[84] The government, in the ElcomSoft and Sklyarov cases, has not argued that AEBPR has been used to do anything illegal other than to violate the anti-circumvention provision, and ElcomSoft claims to know of no circumstance where the program has been used to accomplish any unlawful purpose.[85] The arguments made in ElcomSoft suggest to many that the anti-circumvention provisions of the DMCA, particularly its criminal sanctions, do not strike an appropriate balance between protecting the rights of authors of copyrighted works and the primary purpose of copyright expressed in the Copyright Clause—to promote the public welfare by the advancement of knowledge.[86]

A final issue in this case is whether the anti-circumvention provision changes the "copyright bargain." In an amicus brief filed in support of ElcomSoft's motion to dismiss, the Electronic Frontier Foundation (EFF) and other groups have argued that the DMCA changes the fundamental scope of the copyright protection in the U.S. EFF contends that the copyright laws were enacted to grant authors control over their works to give them incentive to create and distribute new works. But at the same time, the rights granted to authors to control distribu-

82. *See* 17 U.S.C. § 117(a) (2000).

83. *See id.* §§ 107–08.

84. Defendant's Motion to Dismiss Indictment for Violation of Due Process at 4, United States v. Elcom Ltd., No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002).

85. *Id.* at 5–6. According to ElcomSoft, the only uses of AEBPR they know about involve uses of the program to facilitate otherwise legitimate acts: (1) An insurance agent whose eBook stopped working purchased AEBPR after the publisher failed to respond to his requests for help. He was able to convert the eBook, and it now functions properly. (2) A mortgage loan company purchased AEBPR to test the security of PDF encryption to make sure it was secure before placing information on the Internet. (3) The owner of an eBook purchased the program to transfer his eBook from his old to a newly purchased computer.

86. *See* U.S. CONST. art. 1, § 8, cl. 8.

tion of their works are limited in ways that are designed to promote the free flow of ideas and to benefit public education. These limitations on the copyright proprietors' rights—fair use and limited duration of copyrights—are essential to promoting the advancement of knowledge.

The amici argue that the DMCA now eliminates much of the "public side of the copyright bargain"[87] by allowing publishers to exert control over copying works in the public domain and by effectively allowing the copyright owner to prevent digital information from ever entering the public domain because no tools can be made to circumvent an eBook's or other electronic work's protection scheme once the underlying work is in the public domain.[88] The EFF also argues that the government's interpretation of the DMCA in the ElcomSoft case allows publishers to negate fair use because, without access to circumvention technology, no eBook owner can copy even small excerpts or space-shift the book from one computer to another.[89] EFF's brief also warns that an overly broad interpretation of the DMCA allows eBook publishers to effectively eliminate the purchaser's first-sale rights.[90] Under the first-sale doctrine, if a hard copy of a book is sold, the buyer has the right to resell his copy or loan his copy to a friend. Without the ability to move the eBook from one computer to another or to remove the copy from one computer and install it on another, the purchaser of an eBook cannot transfer his copy to another without transferring the computer.

The court did not agree with the amici. The court first found that the DMCA does not negate fair use.[91] It stated:

> Although certain fair uses may become more difficult, no fair use has been prohibited. Lawful possessors of copyrighted works may continue to engage in each and every fair use authorized by law. It may, however, have become more difficult for such uses to occur with regard to technologically protected digital works, but the fair uses themselves have not been eliminated or prohibited.[92]

The court went on to point out that fair users are not guaranteed a right to the most technologically convenient way to engage in fair use.[93] The court also did not accept the argument that the DMCA prevents access to matters in the public domain.[94] The court saw a

87. Amicus Brief of the Electronic Frontier Foundation et al. at 14, *Elcom*, No. CR 01-20138 RMW, 2002 WL 1009662 (N.D. Cal. May 8, 2002).

88. *Id.* at 16.

89. *Id.* at 18.

90. *Id.*

91. Order Denying Defendant's Motion to Dismiss the Indictment on Constitutional Grounds at 18, United States v. Elcom Ltd., No. CR 01-20138 RMW (N.D. Cal. May 8, 2002).

92. *Id.*

93. *Id.* at 18–19.

94. *Id.* at 19.

flaw in this argument in that it presumes that the only available version of a public domain work is an electronic, technologically-protected version:[95]

> To the extent that a publisher has taken a public domain work and made it available in electronic form, and in the course of doing so has also imposed use restrictions on the electronic version, the publisher has not gained any lawfully protected intellectual property interest in the work. The publisher has only gained a technological protection against copying that particular electronic version of the work.[96]

The court also stated that "[p]ublishing a public domain work in a restricted format does not thereby remove the work from the public domain, even if it does allow the publisher to control that particular electronic copy."[97]

VIII. The Lasting Effect of the Anti-Circumvention Provision? *Felton, et al. v. Recording Industry Association of America, Inc.*

The decision by Edward W. Felton and his research team to withdraw their paper, "Reading Between the Lines: Lessons from the SDMI Challenge," from the 4th International Information Hiding Workshop Conference (IHW) brought to light fears that the DMCA might unreasonably chill encryption research as well. Felton and his team cited pressure from the Recording Industry Association of America, Inc. (RIAA) as the reason for their last-minute withdrawal. The end result of the case, however, has been viewed by many as a major victory for the scientific community against overly vigorous application of the statute at the expense of academic freedom.

In September 2000, the Secure Digital Music Initiative (SDMI), a nonprofit corporation in charge of setting security standards for digital copyrighted works, issued a public challenge to test the security of access-control technologies SDMI had designed to protect digital musical recordings. The challenge was to remove a digital watermark—a form of access-control technology—from digital music samples without altering the samples themselves.

Felton and his team, which included scientists from Princeton and Rice Universities, claimed they were able to circumvent at least four of the SDMI technologies in the challenge. Felton's team then reported their findings in a paper they intended to present at the IHW conference. A few weeks before the IHW conference, however, Felton received threatening letters from both RIAA and Verance Corporation, a company responsible for developing some of the technology

95. *Id.*
96. *Id.*
97. *Id.*

involved in the SDMI challenge. Felton's team subsequently withdrew the paper from the IHW conference.

Later that year, Felton and the scientists from his team filed suit in federal district court in New Jersey for declaratory and injunctive relief against both RIAA, Verance and the Attorney General of the United States. The plaintiffs alleged in the suit that they had submitted the paper for publication at the upcoming USENIX Tenth Security Symposium and feared civil and criminal liability.[98] The complaint sought a declaratory judgment that plaintiffs' actions did not violate the DMCA and that the DMCA's anti-circumvention provision violated the First Amendment.[99]

The RIAA moved to dismiss for lack of a justiciable controversy, and the case was ultimately dismissed on that basis.[100] In its motion to dismiss, the RIAA provided assurances that it would not sue the plaintiffs under the DMCA for the presentation and publication of their scientific research.[101] The RIAA advised the court that the threatening positions taken in the letters sent to Felton had long been retracted and that the RIAA had since repeatedly assured both Felton and his team that it had no intentions to sue them under the DMCA.[102] In response to these assurances by the RIAA and Verance, the plaintiffs eventually published the paper with USENIX.[103]

The Attorney General also moved to dismiss, on grounds that the plaintiffs' claims were not ripe because there was no "substantial threat of real harm" because they had neither been prosecuted nor threatened with prosecution under the statute.[104] The defendants argued, and the court accepted their position, that to have a justiciable issue, the plaintiffs must commit to either violating the DMCA or be subject to civil suit or criminal prosecution.[105] In dismissing the case, the court stated that any ruling on the applicability of the statute to

98. Defendant John Ashcroft's Memorandum in Support of Motion to Dismiss at 5, Felton v. Recording Indus. Ass'n of Am., Inc., No. 01-CV-2669 (D.N.J. hearing Nov. 28, 2001).

99. Transcript of Motions Before Honorable Garrett E. Brown United States District Court Judge at 29, Felton v. Recording Indus. Ass'n of Am., Inc., No. 01-CV-2669 (D.N.J. hearing Nov. 28, 2001) (Brown, J.).

100. *Id.* at 30–48 (Brown, J.).

101. *Id.* at 31 (Brown, J.).

102. *Id.* at 32 (Brown, J.).

103. *See id.* at 39 (Brown, J.).

104. Defendant John Ashcroft's Memorandum in Support of Motion to Dismiss at 12–13, Felton v. Recording Indus. Ass'n of Am., Inc., No. 01-CV-2669 (D.N.J. hearing Nov. 28, 2001) (citing Presbytery of the Orthodox Presbyterian Church v. Florio, 40 F.3d 1454, 1462 (3d Cir. 1994)).

105. Transcript of Motions Before Honorable Garrett E. Brown United States District Court Judge at 37, Felton v. Recording Indus. Ass'n of Am., Inc., No. 01-CV-2669 (D.N.J. hearing Nov. 28, 2001) (Brown, J.) ("Here, the plaintiffs have not alleged that they plan to violate the Statute, only that the Statute appears unclear to them. I can't see any credible threat of any imminent prosecution, either civilly or criminally.").

the plaintiffs or the statute's constitutionality in this case would be based on speculation and hypothetical conjecture.[106]

The plaintiffs argued that they had a reasonable apprehension of criminal prosecution because the government had so aggressively enforced the criminal provisions of the DMCA in the Sklyarov case.[107] But the New Jersey court saw a "clear distinction" between Sklyarov's case and Felton's, because ElcomSoft had offered a program specifically designed for circumvention for sale to the general public, whereas Felton and his team had merely published their results to fellow scientists "as part of a scientific process of improving access controls."[108] The court and the Attorney General argued that it was possible that some of the seven exceptions set out in § 1201(d) through (j) of the DMCA might immunize them from liability, but the court found it impossible to tell beyond speculation.[109]

While the defendants and the court were unwilling to concede that the plaintiffs' conduct was immune from the application of the anti-circumvention provision, both the defendants and the court floated the suggestion that the plaintiffs' conduct was not in actual violation of the Act. In explaining its decision, the court stated:

> [i]f you look at the primarily designed language, look at the language in the statute and look at the Attorney General saying this is the way I interpret it, I *certainly can't find any realistic threat of prosecution here whatsoever. . . . Here, plaintiffs' conduct is clearly not covered by the Act which the plaintiffs say is ambiguous.*[110]

A heading from the Attorney General's motion reads: "By Their Own Allegations, Plaintiffs Cannot Reasonably Fear Prosecution Under the DMCA, *As Their Conduct Falls Squarely Outside Its Scope.*"[111]

In any case, the RIAA's and the Attorney General's unwillingness to stand toe-to-toe against the scientific community, which showed strong support for Felton's cause[112]—and against what evidently was a legitimate scientific research study—bodes well for both encryption researchers and critics of the anti-circumvention provision.

106. *Id.* at 34–48 (Brown, J.).

107. *Id.* at 15 (Brown, J.) ("Since the arrest of Mr. Sklyarov, we're not sure where that line [where a violation is found for acting out of commercial advantage or private financial gain] is drawn any longer.").

108. *Id.* at 41 (Brown, J.). "[The plaintiffs] say, as the Attorney General says, by their own allegations, their purpose is not to circumvent any access control measures, but rather to study and assist other [sic] in bolstering those access controls." *Id.* at 44–45 (Brown, J.).

109. *Id.* at 42 (Brown, J.).

110. *Id.* at 46 (Brown, J.) (emphasis added).

111. Defendant John Ashcroft's Memorandum in Support of Motion to Dismiss at 5, Felton v. Recording Indus. Ass'n of Am., Inc., No. 01-CV-2669 (D.N.J. hearing Nov. 28, 2001) (emphasis added).

112. Press Release, Electronic Frontier Foundation, Scientists Support Professor's Copyright Law Challenge (Aug. 13, 2001) (on file with the Texas Wesleyan Law Review).

The *Felton* case raises important questions about the anti-circumvention provision's effect on free speech and scientific research. Commentators have criticized the anti-circumvention provision for the chilling effect it has had and may continue to have on encryption research. They have also questioned how the provision will apply to manufacturers and distributors of technology that could be used for circumvention but that may also have "substantial non-anti-circumvention uses."

Unfortunately, the statute—and the cases to date—do not provide any guidance or definition on what constitutes "primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title" or what constitutes "limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title."

IX. CONCLUSION

The anti-circumvention provision of the DMCA was enacted to balance the interests of copyright owners in protecting their digital works from illegal copying and the rights of legitimate users of copyrighted works. Much controversy has arisen about whether the provision goes too far in protecting the rights of content owners by possibly changing the scope of the copyright protection and treading on First Amendment rights. The anti-circumvention provision has probably had a chilling effect on encryption research in this country, and the U.S. Government's pursuit of criminal sanctions against Russian programmer Sklyarov may curtail public discussion of encryption research in this country. Within the next few years, the courts will likely be faced with many challenges to the anti-circumvention provision of the DMCA. How the courts resolve these challenges will ultimately determine the impact of the anti-circumvention provision on copyright law.