January 2003

What Federal Gun Control Can Teach Us About the DMCA's Anti-Trafficking Provisions

Alfred C. Yen
Boston College Law School, alfred.yen@bc.edu

WHAT FEDERAL GUN CONTROL CAN TEACH US ABOUT THE DMCA'S ANTI-TRAFFICKING PROVISIONS

ALFRED C. YEN*

* Professor of Law, Boston College Law School. Generous comments were provided by Joseph Liu, Glynn Lunney, Michael Madison, and the faculties of Case Western Reserve University Law School, Suffolk University Law School, and Seattle University Law School. The author would like to thank Sheila Bautista, Jerry Marr, Sophia Sasaki, Dan Scales, and Jeff Strom for their help as research assistants. This Article was supported by summer research grants from Boston College Law School.

INTRODUCTION

In July of 2001, Russian computer programmer Dmitry Sklyarov traveled to the United States to speak at a conference in Las Vegas, Nevada. While in Las Vegas, Sklyarov was arrested and charged with violating the Digital Millennium Copyright Act (DMCA).[1] According to the complaint against him, Sklyarov's offense was the writing and distribution of software that enabled translation of documents written in the Adobe Corporation's Secure eBook Format to the more common Portable Document Format (PDF).[2] To the surprise of many, Sklyarov found himself facing a fine of up to $500,000 and up to five years in prison.[3] The federal government held Sklyarov in custody for three weeks before a court released him on $50,000 bail.[4] Sklyarov eventually managed to avoid the charges against him by agreeing to testify against his employer, ElcomSoft.[5]

A little more than a year later, John Allen Muhammad and John Lee Malvo apparently embarked on one of the most notorious shooting sprees in American history, killing ten people and wounding three others in October of 2002.[6] According to news reports and prosecutors, the two men committed these murders with a Bushmaster XM15 rifle, which is a civilian version of the military M16.[7] Many members of the

---

1. Pub. L. No. 105-304, 112 Stat. 2860 (1998). *See Free Dmitry Sklyarov!, at* http://www.freesklyarov.org/background/index.html (last visited Oct. 1, 2003) (on file with the author); *Frequently Asked Questions (and Answers) About the Dmitry Sklyarov & ElcomSoft Prosecution* [hereinafter *Frequently Asked Questions*], Electronic Frontier Foundation, *at* http://www.eff.org/IP/DMCA/US_v_ElcomSoft/us_v_elcomsoft_faq.html#Status (last visited Oct. 1, 2003).

2. United States v. Sklyarov, No. 5-01-257 (N.D. Cal. July 7, 2001), Electronic Frontier Foundation, *at* http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20010707_complaint.html.

3. *Id. See also* 17 U.S.C. § 1204(a) (2000) (establishing penalties for certain violations of the DMCA).

4. *See Free Dmitry Sklyarov!, supra* note 1; *Frequently Asked Questions, supra* note 1.

5. *See* Lisa M. Bowman, *Sklyarov Reflects on DMCA Travails*, CNET NEWS.COM, *at* http://news.com.com/2100-1023-978497.html (last modified Dec. 20, 2002).

6. *See* Carol Morello, Christian Davenport, & Hamil R. Harris, *Pair Seized in Sniper Attacks; Gun in Car Tied to 11 Shootings*, WASH. POST, Oct. 25, 2002, at A1, *available at* http://www.washingtonpost.com/wp-dyn/articles/A14158-2002Oct24.html (last visited Oct. 30, 2003); Josh White & Susan Schmidt, *Capital Murder Charges Filed in Va. Shootings*, WASH. POST, Oct. 29, 2002, at A1.

7. *See* Marsha Kranes, *Sniper's Snapshot; Photo Captures Suspect as Guardsman*, N.Y. POST, Nov. 13, 2002, at 17 (reporting that Muhammad and Malvo used a "commercial version of the military M16"); Mark Shanahan, *Lawsuit Targets Windham Manufacturer of Snipers' Weapon*, PORTLAND PRESS HERALD, Jan. 17, 2003,

public were outraged that such a lethal weapon could be manufactured and sold to civilians.[8] However, Bushmaster's manufacture and sale of the weapon to a Washington gun store were legal as a matter of federal law, and it is unclear how the weapon found its way to Muhammad and Malvo from the gun store.[9]

A casual observer of Sklyarov's plight might wonder how a man who writes a computer program for translating documents from one format to another can face up to a $500,000 fine and five years in jail while a corporation that makes lethal rifles suffers no consequences when one of its weapons is used to kill ten people. Interestingly, the explanation lies—at least partially—in the federal government's stern reaction to the use of digital technology, especially the Internet, to commit copyright infringement.

It has now become commonplace to assert that computer technology challenges copyright. The ease with which computers make and distribute near-perfect copies of digital files over the Internet means that a single person can make a text, song, or movie available to millions of people for no charge.[10] If copyright protects that text, song, or movie, then the owner of the copyright may find that sales of the copyrighted work will suffer.

Not surprisingly, copyright holders sometimes sue those who post or download unauthorized copies of files on the Internet.[11] However,

---

at 1A (reporting that Muhammad and Malvo used a Bushmaster XM15 assault rifle, "which is a civilian version of the military's M16 assault rifle").

8. For example, Senator Charles Schumer stated "'[t]he original assault weapons bill was intended to ban guns like this . . . [b]ut the [National Rifle Association] and their allies managed to put loopholes in the law.'" Bob Port, *It's the All-American Weapon of Death*, N.Y. DAILY NEWS, Oct. 25, 2002, at 10.

9. *See* Steve Miletich, *Families of 2 Sniper Victims File Suit*, SEATTLE TIMES, Jan. 17, 2003, at A1 (reporting that federal authorities did not know how the weapon used to kill the victims was transferred from the gun dealer to Muhammad); Jerry Seper, *No Sales Receipt for Sniper Rifle*, WASH. TIMES, Dec. 8, 2002, at A04 (reporting initial sale of the weapon by Bushmaster to a Tacoma, Washington gun store and investigation by federal authorities into whether the Muhammad and Malvo obtained the rifle through either theft or illegal sale). Legality of the sale under federal law does not necessarily insulate Bushmaster from civil liability that might arise from any negligence on the company's part. However, lawsuits against gun manufacturers for liability associated with shootings have, on the whole, been unsuccessful. *See* Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1860–61 (2000) (noting that gun manufacturers rarely lose strict products-liability actions in cases where there is misusof a gun).

10. *See* Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, 1171 (N.D. Ill. 1997) (describing how uploading a file to a web page made the file available for downloading by Internet users).

11. The best examples of such suits are those filed by the Recording Industry Association of America (RIAA) against individuals who allegedly used the Internet to swap music files. According to the RIAA website, the number of these suits could

such suits face a number of difficulties. Potential defendants may be hard to locate, and they may lack the assets necessary to satisfy a judgment. Additionally, copyright holders in the music, movie, and publishing industries understandably fear adverse business consequences that might come from suing their customers.[12] Accordingly, copyright holders have frequently tried other methods to stop individuals from making copyright holders have frequently tried other methods to stop individuals from making unauthorized copies of files. These efforts have included, among other things, the implementation of encryption schemes known as Digital Rights Management ("DRM") that make the unauthorized viewing or copying of works extremely difficult.[13] This makes sense from the copyright holder's perspective. If CDs, DVDs, and electronic documents cannot be viewed or copied without technology licensed from the copyright holder, then the flow of unauthorized files over the Internet will slow down.

Unfortunately for copyright holders, the DRM technology that protects files can always be breached. Highly publicized cases involving CSS ("Content Scrambler System"—the encryption used to protect DVDs) and Adobe eBook Reader (technology that allows books to be read in digital form and distributed with controls over access and uses such as copying and printing) show that talented members of the public will quickly defeat even elaborate encryption systems.[14] This implies that DRM will be ineffective unless something is done to deny individuals the right and ability to breach DRM.

Not surprisingly, those threatened by the unauthorized distribution of copyrighted works over the Internet have lobbied Congress for such

---

eventually rise into the thousands. The RIAA combined these well-publicized suits with a campaign of "amnesty" for individuals who would admit to file sharing, delete shared files, and promise never to engage in such activity again. *See Recording Industry Begins Suing P2P File Sharers Who Illegally Offer Copyrighted Music Online*, *at* http://www.riaa.com/news/newsletter/090803.asp (last visited Oct. 30, 2003).

12. *See Elderly Man, Schoolgirl, Professor Among File-Swapping Defendants*, *at* http://www.usatoday.com/tech/news/techpolicy/2003-09-09-riaa-defendants_x.htm (last visited Oct. 19, 2003).

13. *See* Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 47-51 (2001) (describing development and use of DRM); Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1093-94 (1998) (describing DRM as a solution to copyright owners' concerns about infringement); Justin Graham, *Preserving the Aftermarket Copyrighted Works: Adapting the First Sale Doctrine to the Emerging Technological Landscape*, 2002 STAN. TECH. L. REV. 1, ¶ 29 nn.83-91 (Aug. 2002), *at* http://stlr.stanford.edu/STLR/Articles/ 02_STLR_1/index.htm (describing various forms of DRM and calling it "the wave of the present and the future").

14. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 435-39 (2d Cir. 2001) (describing circumvention of CSS with software known as "DeCSS"); United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1118 (N.D. Cal. 2002) (describing circumvention of Adobe eBook Reader).

assistance, and Congress has responded. The so-called "anti-trafficking provisions" of the DMCA authorize civil and criminal sanctions against those who sell or distribute technology designed to circumvent encryption schemes.[15] The criminal penalties for willfully violating these provisions are serious. The DMCA punishes a first offense with fines up to $500,000 and five years in prison.[16] A second offense brings fines up to $1,000,000 and ten years in prison.[17] These provisions make it effectively impossible for ordinary individuals to obtain circumvention technology, even if they have a legal use for it.[18]

The imposition of criminal liability on those who distribute circumvention technology is a drastic measure. American law generally does not make someone a felon for supplying technology that has legitimate and legal uses. To be sure, the law sometimes regulates distribution of an item to guard against particular risks.[19] Such action, however, is a far cry from a full-scale ban that makes the item unavailable to people who would use it for lawful purposes. This raises the concern that the DMCA's anti-trafficking provisions are an overreaction to the problem of copyright infringement.

Unfortunately, this problem appears not to have bothered the DMCA's supporters and the lawmakers who passed the statute. Representatives of consumer groups, the public interest, and the electronics industry association appeared before Congress and expressed serious reservations about the effect of the anti-trafficking provisions on

---

15. *See* 17 U.S.C. §§ 1201-1204.

16. The DMCA provides:

> Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain—
> (1) shall be fined not more that $500,000 or imprisoned for not more than 5 years, or both, for the first offense; and
> (2) shall be fined not more than $1,000,000 or imprisoned for not more that 10 years, or both, for any subsequent offense.

Id. § 1204(a).

17. *Id.*

18. *See Elcom*, 203 F. Supp. 2d at 1124 (rejecting criminal defendant's claim that the DMCA anti-trafficking provisions do not apply to the distribution of circumvention technology that can be used for noninfringing purposes); Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 304 (S.D.N.Y. 2000) (rejecting civil defendant's claim that the DMCA's anti-trafficking provisions do not apply to distribution of circumvention technology that can be used for noninfringing purposes).

As this Article will show, there are many lawful uses for circumvention technology. Before passage of the DMCA, circumvention was legal because the copyright code said nothing about circumvention. Even now, the DMCA outlaws circumvention only when accomplished to gain unauthorized access to a copyrighted work. Circumvention for any other purpose therefore remains legal. *See infra* text accompanying notes 24-26; *infra* Part I.C.1 (discussing the legality of circumvention).

19. A few examples of items whose distribution is regulated to curtail risk include alcohol, prescription drugs, and tobacco.

lawful behavior.[20] However, these worries were brushed aside in favor of a statute focused on preventing copyright infringement.[21] Congress apparently bought the argument that copyright infringement on the Internet has become a very serious social problem and that drastic steps are necessary to fight it.[22] Society rightly bans circumvention

---

20. *See WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary*, 105th Cong. 266–67 (1997) [hereinafter *1997 Hearings*] (statement of Gary J. Shapiro, President, Consumer Electronics Manufacturers Association), *available at* http://www.house.gov/judiciary/ 4008.htm; *id.* at 240–49 (statement of Douglas Bennett, President, Earlham College), *available at* http://www.house.gov/judiciary/4015.htm.

21. *See* Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 415–26 (1999) (criticizing the DMCA's anti-trafficking provisions as laws that "sacrific[e] important First Amendment interests for too speculative a gain" (internal quotations omitted)); Burk & Cohen, *supra* note 13, at 51–54 (criticizing the DMCA's anti-circumvention and anti-trafficking provisions as "a rush legally to shore up technological safeguards against such copying, without proper consideration of the policy balance that should animate both legal and technical infrastructures"); Graham, *supra* note 13, ¶ 29 (expressing skepticism about DMCA's anti-trafficking provisions); Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813, 870–81 (2001) (describing overbreadth of DMCA anti-circumvention and anti-trafficking provisions and questioning whether they are needed to preserve incentives for creation); David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 739 (2000) ("The user safeguards so proudly heralded as securing balance between owner and user interests, on inspection, largely fail to achieve their stated goals."); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 522–24 (1999) (characterizing the DMCA's anti-trafficking and anti-circumvention provisions as unbalanced and overbroad).

22. As one court put it:

> Technological access control measures have the capacity to prevent fair uses of copyrighted works as well as foul. Hence, there is a potential tension between the use of such access control measures and fair use. Defendants are not the first to recognize that possibility. As the DMCA made its way through the legislative process, Congress was preoccupied with precisely this issue. Proponents of strong restrictions on circumvention of access control measures argued that they were essential if copyright holders were to make their works available in digital form because digital works otherwise could be pirated too easily. Opponents contended that strong anti-circumvention measures would extend the copyright monopoly inappropriately and prevent many fair uses of copyrighted material.

Reimerdes, 111 F. Supp. 2d at 304 (explaining that Congress may or may not have struck an ideal balance in the DMCA). Individuals representing the interests of copyright holders appeared before Congress to make the case for strong copyright protection. According to some, anything less than the highest level of copyright security would spell tragedy for the United States. For example, Allee Willis, speaking on behalf of Broadcast Music, Inc., stated:

> [W]eak implementing legislation would set a dangerous precedent that would give comfort to our trade competitors and a big boost to foreign pirates. We

> would also make it very unlikely that the Internet will ever reach its full potential as an effective medium for mass entertainment or a broad avenue for scholarly discourse. A legislative framework that sanctions broad exemptions for key players will destroy the fail-safe security that we need to encourage robust commerce on the Net. If Congress builds a loose and open structure, we will: send a signal against self-expression (the power of the song); reduce economic investments in the creation of new works; promote piracy of American music in Cyberspace; and prevent copyright owners from being compensated for the exploitation of their works. The United States will be the big loser.

1997 Hearings, *supra* note 20, at 159–60 (statement of Allee Willis, songwriter, on behalf of Broadcast Music, Inc.), *available at* http://www.house.gov/judiciary/4010.htm; *see also id.* at 128 (statement of Lawrence Kenswil, Executive Vice President, Business and Legal Affairs, Universal Music Group) (outlining danger of copyright infringement associated with new technology), *available at* http://www.house.gov/judiciary/4003.htm. An example of this sentiment's strength was provided by Jack Valenti, President of the Motion Picture Association of America (MPAA), who argued in his statement to a House of Representatives subcommittee that "one of this nation's indispensable objectives must be, has to be, to protect and safeguard intellectual property against pilfering, unauthorized use and illegal copying." *Id.* at 79–80, *available at* http://www.house.gov/judiciary/4011.htm. Mr. Valenti went on to paint an apocalyptic portrait of a world where copyright infringement has run amok over the Internet:

> Internet piracy is not a "maybe" problem, a "could be" problem, a "might someday be" problem. It is a "now" problem. Later, sooner than we think, it could become a cancer in the belly of our business. In odd corners of the World Wide Web, in linked sites based in Europe, Asia and Australia as well as the U.S., a pirate bazaar is underway. Its customers span the globe, wherever the Internet reaches, and its wares are the fruits of American creativity and ingenuity.
>
> Today, Internet piracy focuses on computer programs, video games, and recorded music. Movies and videos are not much in evidence—yet. That's because our audio-visual content is so rich in information that it can't yet move easily everywhere in the digital network—the volume of flow is too great for some of the pipes. We know that the reprieve is temporary, however. The same technology that will smooth the way for legitimate delivery of video on demand over digital networks will also prime the pump for copyright pirates.
>
> MPAA is very familiar with the great video pirate marketplaces of today. In China, in Russia, in Italy, in scores of other countries, video pirates steal more than $2 billion of our intellectual property each year. By spending millions of dollars on anti-piracy campaigns, and with the invaluable help of Congress and of the Executive Branch, MPAA is making great progress in the fight against these pirate cornucopias. I [j]ust recently returned from Russia where in a meeting with the Prime Minister, that nation, urged on by its directors, writers, actors, producers, distributors and businessmen, has endorsed and pledged to support a spacious joint anti-piracy plan led by an amalgam of Russian and American companies. So, even Russia which is literally infested with pirates, has now determined it must now go to war against intellectual property thieves in order to save its own creative industry.

technology to slow down copyright infringement, even if it means that lawful users of such technology must give up some rights.[23]

The argument supporting the DMCA's anti-trafficking provisions is quite plausible, at least on first inspection. A closer analysis, however, reveals some significant weaknesses. Although the anti-trafficking

---

> But we know that the next battleground will be in cyberspace: a virtual pirate shopping mall that—in scope, volume and agility of operation—may dwarf those we are fighting today.
>
> Of one fact you may be certain: The Internet will be the crucial link in the pirate operations of tomorrow. Today, the pirate who obtains, by stealth or malfeasance, a copy of the latest blockbuster picture before it is even released in the theaters must cope with formidable distribution problems. Physical copies must be smuggled across borders, warehoused, and parceled out to distributors before reaching the ultimate consumer. Alas, digital networks will soon make this complex and dangerous undertaking cheap and simple. The pirate master will be digitized, posted on the Web, and made available to Net surfers all over the world. Or, the master will be downloaded over the Internet to a digital video recorder half a world away, that can churn out thousands of pristine, perfect copies at the touch of a button, for immediate distribution to customers. By the time those pirate DVD copies hit the street, the pirate web site will have disappeared, to be set up anew tomorrow in a different country, where a different current hit will be available.

Id. The text of Mr. Valenti's statement offers a fascinating and important glimpse into the motivation behind at least one person's support of the DMCA's anti-trafficking provisions. First, Valenti does not limit his call for action to the prevention of copyright infringement. Instead, he rails against "pilfering, unauthorized use, and illegal copying," a statement that overlooks the fact that copyright law permits a great deal of unauthorized use. *See infra* Part I.A. Although advocates are certainly permitted leeway to make a point, it is not entirely clear that such hyperbole can be dismissed as harmless. The rhetorical effect of Valenti's statement is to sweep legal unauthorized uses into the same category as copyright infringement, and then to claim that all of these things—including unauthorized uses—pose an intolerable threat against which war must be declared. Such a perspective is, at the very least, entirely consistent with a statute that protects copyright, even at the expense of lawful behavior.

23. As the *Elcom* court wrote:

> [W]hile it is not unlawful to circumvent for the purpose of engaging in fair use, it is unlawful to traffic in tools that allow fair use circumvention. That is part of the sacrifice Congress was willing to make in order to protect against unlawful piracy and promote the development of electronic commerce and the availability of copyrighted material on the Internet.

203 F. Supp. 2d at 1125. Jane Ginsburg wrote:

> Congress was persuaded that the relative security of a closed list of exceptions would encourage copyright owners to make works available over digital networks. Were the law to allow leeway for hacking, copyright owners then would lack incentive to offer more varied and less expensive forms of access to and enjoyment of copyrighted works.

Jane C. Ginsburg, *Essay—How Copyright Got a Bad Name For Itself*, 26 COLUM. J.L. & ARTS 61, 70 (2002); *see also* Jack Valenti, Editorial, *There's No Free Hollywood*, N.Y. TIMES, June 21, 2000, at A23 (arguing that society must control technology, especially software that contributes to copyright infringement on the Internet).

measures protect copyright, they do so at the expense of significant rights that the general public is supposed to enjoy. For example, the circumvention of DRM is often perfectly legal.[24] The DMCA generally prohibits circumvention for the purpose of gaining unauthorized access to a work, but it allows people who have legitimately gained access to circumvent other digital controls.[25] The DMCA also permits circumvention for purposes of access in specific circumstances by libraries, law enforcement, software engineers, and encryption researchers.[26] Unfortunately, a person who wants to exercise these rights of legal circumvention will find it practically impossible to do so because the DMCA's anti-trafficking provisions keep her from acquiring the necessary technology. From a policy perspective, this suppression of legal circumvention is troubling because legal circumvention is often tied to noninfringing uses of copyrighted works.[27] The DMCA therefore threatens the long-established balance between copyright's economic incentives for creation and the public's ability to access and use copyrighted works.[28]

A reasonable response to the concerns of the DMCA's critics would be the modification of the DMCA to permit access to circumvention technology for purposes of noninfringing use.[29] Indeed, Congresswoman Zoe Lofgren and Congressman Rick Boucher have introduced separate bills in the House of Representatives along these lines.[30] Unfortunately, neither of these bills presently has a strong chance of passage because the prevailing wisdom frames the debate over circumvention technology in all or nothing terms. According to this wisdom, banning such technology is the only approach that gives copyright holders reasonable security in today's digital world. Circumvention technology is simply too "dangerous" for the general public to handle. If any kind of circumvention technology falls into ordinary hands, then rampant copyright infringement must follow.[31]

---

24. *See infra* Part I.C.1.
25. *See infra* note 79 and accompanying text.
26. *See infra* notes 83–90 and accompanying text.
27. *See infra* Part I.C.2.
28. *See infra* Part I.C.3.
29. *See* Samuelson, *supra* note 21, at 539–46.
30. *See* Press Release, Office of Congresswoman Zoe Lofgren, Lofgren Vows to Protect Consumers in the Fight over Digital Rights Management (Oct. 2, 2002) (announcing introduction of legislation "to protect consumer's ability to enjoy digital copyrighted material"), *at* http://www.house.gov/lofgren/news/2002/021002.htm (on file with author); Internet and Technology Initiatives, U.S. Rep. Rick Boucher, *at* http://www.house.gov/boucher/internet.htm (last visited Oct. 22, 2003) (stating that Representative Boucher introduced legislation "restoring historical balance in copyright law") (on file with author).
31. *See supra* notes 22–23 and accompanying text.

This Article challenges the prevailing wisdom by drawing insight from federal gun control law. Although the relevance of federal gun control to the DMCA might not seem obvious, brief reflection reveals much of value. Both the DMCA and federal gun control use criminal law to curb the misuse of technology. The DMCA attempts to control copyright infringement that occurs when individuals misuse circumvention technology, and gun control laws try to reduce the number of gunshot wounds that occur when individuals misuse guns. In both cases, Congress needs to decide whether the risk of harm to potential victims of technological misuse justifies removing the technology from the hands of people who use it legitimately.

Insight arises from this comparison because the regulatory approach of federal gun law differs sharply from the approach of the DMCA.[32] As has already been noted, the DMCA operates on the premise that a compromise between the security of copyright and the legal use of circumvention technology is impossible. The risk of copyright infringement is too high, so the public must give up the lawful use of circumvention technology. By contrast, federal gun control operates on the premise that a compromise between the elimination of gun violence and the lawful use of guns is necessary.[33] Federal gun laws, therefore, permit the regulated sale of guns even though such sale exposes the public to the possibility of gun violence.[34]

---

32. It is worth emphasizing that this Article does not take a position about the normative desirability of gun control, nor does it argue that any particular regime of circumvention technology control is desirable simply because a similar regime exists in gun control. Instead, the Article uses gun control law as a source of ideas about how to control the availability of technology while preserving reasonable access for lawful purposes.

33. Consider, for example, the statement of purpose found in the Gun Control Act of 1968—arguably the most stringent federal gun control law ever passed:

> The Congress hereby declares that the purpose of this title is to provide support to Federal, State, and local law enforcement officials in their fight against crime and violence, and it is not the purpose of this title to place any undue or unnecessary Federal restrictions or burdens on law-abiding citizens with respect to the acquisition, possession, or use of firearms appropriate to the purpose of hunting, trapshooting, target shooting, personal protection, or any other lawful activity, and that this title is not intended to discourage or eliminate the private ownership or use of firearms by law-abiding citizens for lawful purposes, or provide for the imposition by Federal regulations of any procedures or requirements other than those reasonably necessary to implement and effectuate the provisions of this title.

Pub. L. No. 90-618, § 101, 82 Stat. 1213, 1214, (1968) (codified at 18 U.S.C. § 921). *See also* Firearms Owners' Protection Act, Pub. L. No. 99-308, § 1, 100 Stat. 449 (1986) (amending 18 U.S.C. § 921) (identifying the need for additional legislation to protect the ability of law-abiding citizens to acquire and use guns for lawful purposes).

34. *See infra* Part II.

The compromise approach of federal gun control implies that the prevailing wisdom about circumvention technology is wrong. If federal gun law can strike a compromise between public safety and lawful uses of guns, then the DMCA should be able to strike a similar compromise between the security of copyright and lawful uses of circumvention technology. As this Article will show, federal gun law contains a number of specific regulatory techniques that can be borrowed to improve the DMCA. These borrowed techniques include: licensing those who make and sell circumvention technology; recording the identities and addresses of those who buy circumvention technology; restricting the form and function of circumvention technology; restricting the methods by which circumvention technology is sold; prohibiting sales to minors; and imposing a series of graduated penalties for violating distribution controls or using circumvention technology to commit serious forms of copyright infringement.

This Article combines these techniques to identify the contours of a more reasonable circumvention technology law. This proposal offers security to copyright holders by imposing accountability on those who might contribute to misuse of circumvention technology by blocking the channels of distribution most likely to place circumvention technology in the hands of irresponsible users, by banning the most dangerous forms of circumvention technology, and by prohibiting the sale of circumvention technology to those most likely to misuse it. Significantly, however, these techniques also allow most people to obtain circumvention technology for lawful purposes. Implementation of these techniques would therefore improve the DMCA.

The Article proceeds in four Parts. Part I describes the DMCA's treatment of circumvention technology against a backdrop of copyright's traditional balance between incentives for creation of works and public rights of access and use. Part II studies federal gun control law to see what themes govern its moderate regulation of guns. Part III uses federal gun control law to suggest a similarly moderate approach to the regulation of circumvention technology. Finally, Part IV evaluates this moderate approach and discusses how it improves the DMCA.

I. COPYRIGHT'S BALANCE AND THE ANTI-TRAFFICKING PROVISIONS

A. Copyright's Balance

The DMCA's anti-trafficking provisions are best understood against the backdrop of copyright as it existed before the DMCA. That law embodies a series of compromises between the interests of copyright holders and the public that the DMCA purportedly leaves undisturbed.[35] These compromises give incentives to authors for the production of creative works while ensuring public access and use. This balance is part of a constitutional scheme that recognizes copyright's potential costs and benefits in a culture that values free speech and civil liberties.

The Constitution authorizes Congress to pass copyright legislation of limited duration and scope. Article I of the Constitution links copyright to the specific purpose of promoting "science and the useful arts" and limits the duration of copyright.[36] Additionally, the First Amendment prevents copyright from expanding to the point that it unconstitutionally restricts free speech.[37] A limited monopoly,

---

35. The DMCA states that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." 17 U.S.C. § 1201(c)(1). It further states that "[n]othing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products." § 1201(c)(4).

36. U.S. CONST. art. I, § 8, cl. 8 ("The Congress shall have the Power . . . . To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.").

37. As a matter of structural logic, the First Amendment has to limit all provisions contained in Article I of the Constitution. Although the Supreme Court has never held any piece of copyright legislation unconstitutional for First Amendment reasons, the Court has recognized the First Amendment's importance to copyright. *See* Eldred v. Ashcroft, 123 S. Ct. 769, 788-90 (2003) (implying that the general shape of copyright law is consistent with the First Amendment, but also rejecting lower court statement that copyright is "categorically immune" from First Amendment scrutiny); Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985) (noting how copyright doctrines such as fair use and the idea/expression dichotomy keep copyright from running afoul of the First Amendment). A significant body of academic scholarship supports this recognition and suggests that courts understate the importance of the First Amendment to copyright law. *See generally* C. Edwin Baker, *First Amendment Limits on Copyright*, 55 VAND. L. REV. 891 (2002); Benkler, *supra* note 21; Robert C. Denicola, *Copyright and Free Speech: Constitutional Limitations on the Protection of Expression*, 67 CAL. L. REV. 283 (1979); Paul Goldstein, *Copyright and the First Amendment*, 70 COLUM. L. REV. 983 (1970); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147 (1998); Neil Weinstock Netanel, *Locating Copyright Within the First Amendment Skein*, 54 STAN. L. REV. 1 (2001) (analyzing relationship between copyright law and the First Amendment); Melville B. Nimmer, *Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press?*, 17 UCLA L. REV. 1180 (1970); L. Ray Patterson, *Free Speech, Copyright, and Fair Use*, 40 VAND. L. REV. 1 (1987);

therefore, forms the heart of copyright.[38] Section 106 of the Copyright Act reserves to copyright owners the exclusive right to reproduce their works, to prepare derivative works based on their works, to distribute copies of the work, to perform the work publicly, to display the work, and to perform the work publicly by means of digital audio transmission.[39] Together, these exclusive rights give potential authors the incentive to create new works by preventing others from free riding on the author's creative labor. If copyright did not exist, then authors of new books might worry that competitors would simply print and sell copies of the book for less than the author, because competitors would not have to incur the cost of writing the book. The reservation of reproduction rights to the author means that those who wish to print the book will have to seek permission from the author and pay a royalty if the author so desires.

The benefits of copyright's existence do not, however, justify a complete monopoly for copyright owners because monopolies do not normally serve the public interest. As a matter of general economics, monopolists restrict output and charge higher prices for their goods.[40] The legal system therefore resists monopolization through the application of antitrust law.[41] In the case of copyright, society sensibly tolerates the costs of monopolies as the price paid to induce the creation of valuable works, but it must limit the scope of those monopolies to prevent copyright from imposing unproductive and frankly absurd restrictions on the use and production of creative works.[42] Copyright, therefore, gives the public substantial rights that limit the scope of copyright.

Pamela Samuelson, *Reviving* Zacchini: *Analyzing First Amendment Defenses in Right of Publicity and Copyright Cases*, 57 TUL. L. REV. 836 (1983); Lionel S. Sobel, *Copyright and the First Amendment: A Gathering Storm?*, 19 COPYRIGHT L. SYMP. (ASCAP) 43 (1971); Alfred C. Yen, *A First Amendment Perspective on the Idea/Expression Dichotomy and Copyright in a Work's "Total Concept and Feel"*, 38 EMORY L.J. 393 (1989); Diane Leenheer Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 WM. & MARY L. REV. 665, 666 (1992) (discussing understatement of conflict between copyright and the First Amendment).

38. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 429 (1984) ("The monopoly privileges that Congress may authorize are neither unlimited nor primarily designed to provide a special private benefit. Rather, the limited grant is a means by which an important public purpose may be achieved.").

39. 17 U.S.C. § 106.

40. *See* ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 38, 250 (2d ed. 1997) (describing behavior of monopolists and their effect on the economy); HARVEY F. ROSEN, PUBLIC FINANCE 53 (1995).

41. *See* 15 U.S.C. § 2 (imposing punishment on those who attempt to monopolize any industries or trades).

42. *See Sony*, 464 U.S. at 432–33 (noting limits on scope of copyright are necessary to advance copyright's purpose).

Among other things, copyright does not protect facts, ideas, concepts, processes, and principles—even if they are part of a work protected by copyright.[43] Copyright protection lasts for only a limited number of years.[44] Those who lawfully purchase copyrighted works are free to dispose of their copies as they see fit.[45] Copyright holders are sometimes compelled to grant licenses to those who want to use their works.[46] And, perhaps most important of all, many uses that would otherwise infringe upon the exclusive rights of copyright holders are permitted as fair use, especially when the use is educational, critical, or non-profit, and does not unduly affect the market for the copyrighted work.[47]

It is important to understand that public rights of use and access do more than blunt the undesirable economic effects of copyright monopolies. These rights keep copyright within its constitutional boundaries, and they also help maintain an appropriate relationship between people and the books, music, and movies that society produces. Although it is impossible to identify an optimal regime of copyright, it is possible to explain the constitutional and social importance of balancing copyright rights with significant users' rights.

If copyright reserved *every* use of a work for the copyright holder, then many everyday behaviors that people take for granted would become violations of federal law. A person coming across an abandoned newspaper in a coffee shop would break the law if she began reading it.[48] People would need permission to load their music CDs onto an MP3 player[49] or make archival copies of works they have

---

43. 17 U.S.C. § 102(b).

44. *Id.* §§ 302-304.

45. *Id.* § 109(a) ("Notwithstanding the provisions of section 106(3), the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord.").

46. *See id.* § 115 (ereating a compulsory license for the making of phonorecords); *id.* §§ 119, 122 (establishing a statutory scheme of mandatory licensing and royalty payments affecting satellite and cable television transmission of copyrighted works).

47. *Id.* § 107 (codifying the fair use doctrine); *see also Sony*, 464 U.S. at 449 & n.32 (establishing fair use for home recording of television programs for later viewing); Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 594 (1994) (recognizing fair use defense for parody).

48. A law that reserved *every* use of a work to a copyright holder would include a right to control reading of the copyrighted work. No such reservation presently exists in the copyright code.

49. The loading of CDs onto an MP3 player for purposes of private, noncommercial listening is likely a fair use under 17 U.S.C. § 107 (codifying the fair use doctrine) or a noninfringing use under § 1008, which prohibits infringement actions "based on the noncommercial use by a consumer" of a digital or analog recording device. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., 180 F.3d

purchased to guard against damage to digital files.[50] Book reviewers would not be able to use short quotes to illustrate their opinions.[51] No one could write new mystery novels in which "the butler did it."[52] Consumers would break the law if they recorded their favorite television shows for later viewing.[53] Libraries would need permission from publishers to lend books.[54] People would have to pay to sing in the shower,[55] as would teachers when showing films to their students.[56]

Fortunately, existing law permits each of these uses and many others.[57] A copyright code that prohibited them would profoundly change society by giving copyright holders the power to stop or demand payment for everyday uses that people presently enjoy. In short, an extremely broad copyright code would give copyright holders an inordinate amount of control over the reading, listening, and viewing habits of the general public. Totalitarian states use control over reading, listening, and viewing habits to maintain the power they wield over their populations. Giving that control to copyright holders is, at the very least, risky—especially when those who hold important copyrights gain

---

1072, 1079 (9th Cir. 1999) (stating in dicta that consumer loading of music onto MP3 players is consistent with congressional intent to permit consumer copying for private, noncommercial use and citing with approval the leading fair use case of *Sony Corp. of America v. Universal City Studios*, 464 U.S. at 455).

50. The making of archival copies is also likely fair use. *See Elcom*, 203 F. Supp. 2d at 1135 ("making a back-up copy of an ebook, for personal noncommercial use would likely be upheld as a non-infringing fair use").

51. Such behavior is presently considered fair use. *See* 17 U.S.C. § 107 (listing criticism and comment as two forms of fair use); *see also Campbell*, 510 U.S. at 591–92 (noting that lack of market for critical borrowing removes the likelihood of licensing for such use, thereby implying that such borrowing is fair use).

52. The copyright code does not presently stop one author from borrowing the ideas of another. *See* 17 U.S.C. § 102(b) (denying copyright protection to ideas contained in works); *see also* Nichols v. Universal Pictures Corp., 45 F.2d 119, 121–22 (2d Cir. 1930) (leading case describing the distinction between idea and expression and denying plaintiff's claim that general similarities of plot and subject matter constituted copyright infringement).

53. The Supreme Court considered and rejected a claim that such behavior is infringement. *See Sony*, 464 U.S. at 456 (holding that such time-shifting is fair use).

54. The present copyright act does not give copyright holders the power to control secondary sale or distribution of their works. *See* 17 U.S.C. § 109(a) (codifying the first sale doctrine, which permits a lawful owner of a book to dispose of possession without the authority of the copyright holder).

55. Such use might belong to a copyright holder if the right of performance extended to all performances, public or private. However, copyright law gives copyright holders only the exclusive rights over public performances. *Id.* § 106(4) (granting exclusive right of public performance to copyright holder).

56. Such a screening might be considered a public performance, but 17 U.S.C. § 110(1) specifically exempts performances by teachers in a face-to-face classroom setting. *Id.* § 110(1).

57. *See supra* notes 49–56 and accompanying text.

wealth that can be used to influence government.[58] Accordingly, it is important for Congress to ensure that the copyright statute does not give copyright holders an inappropriate amount of control over their works.

B. Anti-trafficking: An Elegant Solution to Digital Copyright Infringement?

The DMCA's anti-trafficking provisions are a response to the common misuse of digital technology, especially the Internet, for purposes of copyright infringement.[59] The Internet arose as a U.S. Department of Defense project and has evolved into a network linking computers from around the world.[60] Anyone with a personal computer can join this network, which permits very rapid communication with millions of other users. A person connected to the Internet can therefore send and receive data files that embody music, books, and movies.[61]

The Internet has proven revolutionary because it makes the efforts of one person instantaneously available to millions of others. This is, on the whole, a marvelous blessing. Those who have items to share with the rest of the world can now do so inexpensively and effectively. For example, a person anxious to share his opinions about the Boston Red Sox no longer needs a newspaper or other media institution to publish his writings. Instead, he can post it to a web page where others can read it. Businesses can establish web sites that promote their products twenty-four hours a day. To the extent that those businesses sell items such as books or music that can be converted to digital formats, they can

---

58. *See* Marci A. Hamilton, *Farewell Madison Avenue*, 16 CONST. COMMENT. 529, 532-33 (1999) (criticizing the extension of copyright terms by twenty years "mainly because Disney lobbied like crazy to keep their images from falling into the public domain"); Jon M. Garon, *Media & Monopoly in the Information Age: Slowing the Convergence at the Marketplace of Ideas*, 17 CARDOZO ARTS & ENT. L.J. 491, 522-24 (1999) (describing the economic interests that motivated large copyright holders to lobby Congress for additional copyright protection).

59. *See Corley*, 273 F.3d at 435. The court in Corley stated:

> Fearful that the ease with which pirates could copy and distribute a copyrightable work in digital form was overwhelming the capacity of conventional copyright enforcement to find and enjoin unlawfully copied material, Congress sought to combat copyright piracy in its earlier stages, before the work was even copied.

Id.

60. For a brief history of the Internet, see Barry M. Leiner et al., *A Brief History of the Internet*, *at* http://www.isoc.org/internet/history/brief.shtml (last visited Oct. 30, 2003). For a more extensive treatment of the subject, see Jay P. Kesan & Rajiv C. Shah, *Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System*, 79 WASH. U. L.Q. 89 (2001).

61. *See also Marobie-FL*, 983 F. Supp. at 1171 (describing how uploading a file to a web page made the file available for downloading by Internet users).

use the Internet to deliver those items instantaneously to the purchaser. The Internet, therefore, has the potential to foster and support a rich, vibrant marketplace for digital works.

Despite the promise of a digital marketplace, digital technology frightens copyright holders. It frightens them because digital technology makes it possible for individuals to commit copyright infringement or otherwise interfere with a copyright holder's attempt to sell her works over the Internet. Consider a website that transmits a digital copy of a song to users upon payment of a fee. Even though the website is programmed not to transmit the song until the proper fee has been paid, some individuals may develop the ability to trick the website into believing that the fee has been paid. The copyright holder could fight this practice by encrypting the song file so that the unauthorized recipient cannot hear it. Once again, however, enterprising individuals will likely figure out how to circumvent the encryption and gain access to the work.

The problem of making sure that people pay for copies of copyrighted works is undoubtedly serious, but copyright holders worry even more about what people might do after they buy copies of works. People who have purchased a work can easily copy the relevant files to the hard drives of their personal computers. From there, it is easy to make those files available to millions of people over the Internet. As phenomena like Napster and Kazaa make clear, there are enough people willing to do this so that a very rich collection of works will be constantly available on the Internet for free downloading.[62] In theory, copyright holders could impose DRM schemes that make it impossible to copy a work without permission, but here too one or more individuals will probably figure out how to circumvent the relevant protection. These individuals could then distribute circumvention technology as software to millions over the Internet. Accordingly, providers of intellectual property understandably fear that the Internet will ruin the profitability of their copyright monopolies. After all, why would anyone buy a legitimate copy of something when she could download it for free over the Internet?

As of this writing, traditional legal methods have had relatively limited success in stopping copyright infringement on the Internet. So far, copyright owners have not sued enough ordinary individuals to deter

---

62. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011–13 (9th Cir. 2001) (describing operation of Napster and availability of music files on the Internet via Napster); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1032–33 (C.D. Cal. 2003) (describing operation and effect of peer-to-peer systems); *see also* Kenneth Terrell & Seth Rosen, *A Nation of Pirates,* U.S. NEWS & WORLD REP., July 14, 2003, at 40, 42–43 (describing file trading over peer-to-peer networks).

others from infringing.[63] This is not to say that copyright holders have done nothing. Copyright holders have sued companies like Napster and Kazaa who provide file swapping technology or services.[64] However, these efforts have not been particularly successful at stopping infringement because recent versions of such technology are not operated by a single entity that can be closed by court order.[65] Instead, they operate simultaneously on numerous computers operated by people who are not parties to the cases brought in court. In some cases, those people may also be beyond the reach of the court because they reside in foreign countries. Copyright holders have also pursued action through the Internet Service Providers (ISPs) that provide Internet access to infringers, but with less success. As a general rule, courts have correctly refused to hold ISPs financially liable for copyright infringement committed by their users.[66] Nevertheless, copyright holders have generally been able to get ISPs to remove infringing material from the Internet upon complaints from copyright holders.[67] However, ISPs have not yet agreed to actively police the Internet for infringement or disable the use of Internet applications that might be used to commit infringement, and for good reason. Many of the most popular applications used to swap infringing files can also be used to swap noninfringing files. ISPs understandably worry about curtailing

---

63. There are a number of plausible explanations for this. It is often difficult to determine the identity of people using the Internet. Ordinary individuals often do not commit offenses that are serious enough to support the expenses of litigation, nor do they have the funds to satisfy any large judgments that might be obtained. Large copyright businesses may also shrink from highly publicized actions against ordinary individuals because they fear negative fallout that might come with suing their customers. However, the practice of not suing individuals who share copyrighted material over the Internet may be changing, as the RIAA has begun a campaign to sue a number of individuals who have engaged in this behavior. *See supra* note 11.

64. *See Napster*, 239 F.3d at 1011 (affirming preliminary injunction against Napster); *Grokster*, 259 F. Supp. 2d at 1031 (denying defendants' motion to dismiss).

65. *See Grokster*, 259 F. Supp. 2d at 1039-40 (describing decentralized operation of certain peer-to-peer networks).

66. *See* Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361, 1372-73 (N.D. Cal. 1995) (expressing skepticism about the possibility of holding ISPs liable for the users' acts of infringement); *see also* Yen, *supra* note 9, at 1838-81 (analyzing legal issues surrounding potential liability of ISPs for user copyright infringement).

67. The copyright code now contains a "safe harbor" provision that provides limited protection to ISPs from liability for user copyright infringement. ISPs who want to take advantage of the safe harbor must designate an official agent to receive complaints of copyright infringement from copyright holders and promptly remove or disable access to allegedly infringing material found on the ISP's system. This amounts to limited immunity in exchange for cooperating with complaining copyright holders. *See* 17 U.S.C. § 512(c) (providing ISPs with limited protection against liability for user infringement); *see also* Yen, *supra* note 9, at 1885-89 (analyzing and evaluating the safe harbor provisions concerning ISP liability for user infringement).

the legal activities of their users. Moreover, they do not want to become "Internet police."

The problems outlined above have caused many copyright holders to explore self-help as a method for curtailing infringement. This strategy has become possible because distributors of digital files can now encrypt them to limit and manage the ways that people can use them. When used systematically, this type of DRM allows the distributor of a digital work to control whether a particular person can read a work, limit the number of times a work is read, prohibit printing, and prevent digital copying.[68]

In theory, DRM should greatly reduce copyright infringement. However, a fly in the ointment remains. Copyright holders can impose DRM on consumers, but they cannot stop consumers from defeating DRM. It is a simple fact of the digital age that any DRM scheme can be broken by enterprising individuals who will share their knowledge or technology, sometimes over the Internet for free. Accordingly, DRM is unlikely to work as a solution to copyright infringement unless something is done to suppress the public's ability to defeat DRM schemes. Otherwise, copyright holders may face a doomsday scenario in which software that defeats all of their DRM schemes can be downloaded from the Internet free of charge.[69]

The DMCA's anti-trafficking provisions play a major role in the legislative solution to this problem.[70] As will be described in more detail below, these provisions outlaw the sale or distribution of services and technology necessary to defeat DRM. This supports the technical self-help measures that copyright holders use by making it harder for ordinary people to commit copyright infringement with digital technology. To be sure, enterprising individuals will still develop methods for defeating digital controls on copyrighted works, but they cannot share their skill or technology without breaking the law.[71]

At first inspection, the anti-trafficking provisions come across as an elegant solution to a difficult problem. If copyright infringement is running rampant on the Internet, then why not curtail it by making it impossible for people to defeat self-help measures? However, closer inspection complicates this appearance of elegance. The DMCA

---

68. *See* Burk & Cohen, *supra* note 13, at 48–50; Graham, *supra* note 13, ¶¶ 29–30.

69. *See Reimerdes*, 111 F. Supp. 2d at 315 (stating that the availability of DeCSS over the Internet effectively compromised the value of the encryption scheme used to protect DVDs).

70. *See* Benkler, *supra* note 21, at 416–17 (characterizing the anti-trafficking provisions as more important than provisions directed at the actual practice of circumvention); Samuelson, *supra* note 21, at 554–55.

71. *See* 17 U.S.C. § 1201(a)–(b); *see also infra* text accompanying notes 75–77.

suppresses copyright infringement, but it also interferes with the public's ability to exercise a number of lawful rights of access to and use of copyrighted works. If the lost rights are insignificant, then it may still be appropriate to consider the DMCA's anti-trafficking provisions elegant. But, if the lost rights are important, then the DMCA's anti-trafficking provisions become an instrument that upsets copyright's balance.

C. An Analysis of the DMCA's Anti-trafficking Provisions

The DMCA splits the world of DRM and circumvention into two categories: "access control" and "use control."[72] The term "access control" refers to technology that prevents an unauthorized person from viewing the contents of a particular digital file. For example, CSS makes it impossible for someone to watch the movie unless they have a DVD player equipped with licensed technology that can read the CSS-protected file.[73] By contrast, "use control" refers to technology that prevents unauthorized use of a file *after* a person has already gained access. For example, Adobe's eBook Reader (the DRM system that Dmitri Sklyarov's software defeated) allows the copyright holder to keep the reader of an electronic book (a person who already has access to the work) from copying the book or reading it on more than one computer.[74] It is, of course, possible to implement DRM that has both access-control and use-control features.

The DMCA's anti-trafficking provisions outlaw the sale and distribution of technology that circumvents access controls or use controls. 17 U.S.C. § 1201(a)(2) applies to access controls. It provides:

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

---

72. *Compare* 17 U.S.C. § 1201(a) (referring technological measures that effectively control "access" to a copyrighted work), *with id.* § 1201(b) (referring to technological measures that effectively control "a right of a copyright owner"). *See also Elcom*, 203 F. Supp. 2d at 1119–20 (distinguishing DRM measures that control access to works from those that control the use of works).

73. *Reimerdes*, 111 F. Supp. 2d at 303.

74. *Elcom*, 203 F. Supp. 2d at 1117–18 (describing operation of Adobe eBook Reader).

> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.[75]

A second provision, 17 U.S.C. § 1201(b)(1) contains almost identical language with respect to use controls:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing 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;
>
> (B) has only limited commercially significant purpose or use other than to circumvent 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; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing 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.[76]

For purposes of this Article, it is important to measure the effect of the above-quoted provisions on the public's ability to access and use various works. Their impact is clear: selling circumvention technology is against the law, even if the purchaser uses it for a noninfringing purpose.[77] The DMCA therefore has the practical effect of suppressing

---

75. 17 U.S.C. § 1201(a)(2).

76. *Id.* § 1201(b)(1).

77. Commentators who first analyzed the DMCA thought that courts might interpret the statute narrowly, leaving room for the distribution and use of circumvention technology for noninfringing purposes. *See* Nimmer, *supra* note 21, at 741 (noting that

at least some public rights of access and use, namely those that involve noninfringing circumvention of DRM. The question is, of course, the number and importance of the rights that get suppressed. If these rights are few and insignificant, then the anti-trafficking provisions would seem relatively uncontroversial. This would be the case if Congress has declared circumvention generally illegal, or if instances of noninfringing circumvention are very rare.

By contrast, if the DMCA suppresses meaningful instances of noninfringing access and use, then the anti-trafficking provisions become problematic. Any free society should look warily upon a legal scheme that explicitly gives people rights only to take them away by outlawing the means of exercising those rights. Such concern makes particular sense in the case of the DMCA's anti-trafficking provisions because the DMCA itself provides that "[n]othing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."[78] Accordingly, this Article next considers the general legality of circumvention and the relationship between circumvention and copyright infringement. As will be shown, circumvention is generally legal, and accordingly, the DMCA burdens significant rights of public access and use.

1. ANTI-TRAFFICKING AND THE LEGALITY OF CIRCUMVENTION

The DMCA's anti-trafficking provisions may outlaw the sale of circumvention technology, but circumvention itself is generally legal. 17 U.S.C § 1201(a)(1)(A) contains the sole specific prohibition against

---

courts might need to limit the breadth of the DMCA's anti-circumvention and anti-trafficking laws by narrow interpretation or the application of constitutional limits); Samuelson, *supra* note 21, at 544–46 (calling for narrow interpretation of the DMCA's anti-circumvention and anti-trafficking provisions). However, courts have shown absolutely no inclination to interpret the anti-trafficking provisions as suggested. In the only criminal case litigated as of this writing, the Northern District of California analyzed 17 U.S.C. § 1201(b) as follows:

> In short, the statute bans trafficking in any device that bypasses or circumvents a restriction on copying or performing a work. Nothing within the express language would permit trafficking in devices designed to bypass use restrictions in order to enable a fair use, as opposed to an infringing use. The statute does not distinguish between devices based on the uses to which the device will be put. Instead, all tools that enable circumvention of use restrictions are banned, not merely those use restrictions that prohibit infringement. Thus, as the government contended at oral argument, Section 1201(b) imposes a blanket ban on trafficking in or the marketing of any device that circumvents use restrictions.

Elcom, 203 F. Supp. 2d at 1124. *See also Reimerdes*, 111 F. Supp. 2d at 304 (rejecting defendant's claim in a civil case that the DMCA's anti-trafficking provisions should not apply because users could use circumvention technology for noninfringing purposes).

78. 17 U.S.C. § 1201(c)(1).

circumvention, but it applies only to the circumvention of access controls. This application makes the circumvention of use controls legal.[79] Moreover, it turns out that even the circumvention of access controls is sometimes legal as well.

Consider first the language from § 1201(a)(1)(A) that outlaws circumvention of access controls. That section provides that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title."[80] This language confines the prohibition against circumvention to cases involving a work protected by copyright. People therefore have the right to circumvent DRM that protects access to public domain works. This right includes works that have never been protected by copyright such as the white pages of the telephone book[81] and works whose copyright has expired.[82]

Sections 1201(a)(1)(B) and (C) and 1201(d) through (j) contain a series of specific exceptions that permit circumvention otherwise prohibited by § 1201(a).[83] Section 1201(d) allows nonprofit libraries and educational institutions to circumvent DRM in certain situations in order to examine a work for purposes of deciding whether to purchase a copy of that work.[84] Section 1201(e) exempts certain activities of state and federal government, including law enforcement and intelligence gathering.[85] Section 1201(f) permits circumvention for purposes of achieving interoperability between two computer programs.[86] Section 1201(g) allows circumvention when necessary for encryption research.[87] Section 1201(i) gives people the right to circumvent in limited circumstances when they are protecting their privacy.[88] Section 1201(j) exempts security testing from the reach of § 1201(a)(1)(A).[89] Finally, § 1201(a)(1)(B) and (C) create an administrative process that allows circumvention for particular classes of works identified by the Register of Copyright as works for which noninfringing uses as "adversely affected" by § 1201(a)(1)(A)'s prohibition of circumvention.[90] So far, the Register has identified two such classes of works: "(1) Compilations

---

79. *See Elcom*, 203 F. Supp. 2d at 1120 ("Unlike Section 1201(a), however, Congress did *not* ban the act of circumventing the use restrictions.").

80. 17 U.S.C. § 1201(a).

81. *See* Feist Publ'ns, Inc. v. Rural Tel. Co., Inc., 499 U.S. 340, 363-64 (10th Cir. 1991) (holding that copyright does not protect a "white pages" telephone directory).

82. *See* 17 U.S.C. §§ 302-303 (establishing length of copyright term).

83. *Id.* § 1201.

84. *Id.* § 1201(d).

85. *Id.* § 1201(e).

86. *Id.* § 1201(f).

87. *Id.* § 1201(g).

88. *Id.* § 1201(i).

89. *Id.* § 1201(j).

90. *Id.* § 1201(a)(1)(B)-(C).

consisting of lists of websites blocked by filtering software applications; and (2) Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsoleteness."[91]

The foregoing shows that many, if not most, instances of circumvention are perfectly legal. Accordingly, the DMCA's anti-trafficking provisions cannot be supported with the claim that circumvention is already prohibited by law. It also follows that the anti-trafficking provisions effectively force people to give up many instances of legal circumvention by eliminating the technology required to exercise that right. Accordingly, the anti-trafficking provisions are unproblematic only if legal acts of circumvention generally lead to copyright infringement.

2. ANTI-TRAFFICKING, THE PUBLIC DOMAIN, AND COPYRIGHT INFRINGEMENT

Without question, circumvention facilitates copyright infringement. However, circumvention is clearly distinct from infringement. Section 106 of the copyright code lists the exclusive rights granted to copyright holders. Those rights include the right to reproduce the copyrighted work, prepare derivative works, distribute copies of the work, publicly perform the work, and publicly display the work.[92] A person who circumvents technical protection of a work does not reproduce, distribute, publicly perform, publicly display, or make derivative works from the work in question. Circumvention means only that the circumventing party has disabled technology that would otherwise prevent unauthorized access to or use of the work.

A circumventer, therefore, does not necessarily commit infringement. Such a person may be intent only upon exercising one of the many rights of access and use that the public is supposed to enjoy.[93] Accordingly, the DMCA's ban against such technology necessarily suppresses noninfringing uses as well as infringing ones because the ban affects all forms of circumvention. It is important, therefore, to determine the number and importance of the noninfringing uses burdened by the DMCA's anti-trafficking provisions. As this Section will show, these rights are important enough to raise questions about the wisdom of the DMCA's approach to circumvention technology.

---

91. 37 C.F.R. § 201.40(b)(1)-(2) (2002).
92. 17 U.S.C. § 106.
93. *See supra* notes 47-55 and accompanying text.

a. Anti-trafficking and Access to the Public Domain

As an initial matter, it is important to understand that the DMCA's anti-trafficking provisions diminish access to and use of public domain works by helping publishers of digital content protect more than they are entitled to receive under the copyright code. Overprotection happens because there is nothing that requires publishers to limit DRM to the defense of copyright rights. Distributors of digital content can apply DRM to control public domain material and noninfringing uses of copyrighted works.

Consider what happens when publishers apply DRM to a work from the public domain.[94] Consumers are clearly entitled to circumvent this DRM because the work in question is not protected by copyright. However, the anti-trafficking provisions will probably prevent the sale of technology to defeat the DRM because publishers likely will use the same DRM scheme to protect works not in the public domain. If this is the case, then the DMCA's anti-trafficking provisions forbid anyone from selling technology to defeat the DRM because the technology would be "primarily designed or produced for the purpose of circumventing protection."[95] Even if a technology provider were prepared to argue that the defeating technology was designed solely to circumvent DRM on public domain works, the risk of an adverse finding is sufficiently high to discourage all but the bravest technology providers.[96]

---

94. For example, Herman Melville's *Moby Dick* is available for sale in a number of different formats at www.ebookmall.com. According to the website, some of these formats (e.g., Microsoft Word, plain text, and Adobe PDF) allow printing of the text, while other formats (Adobe eBook Reader and Microsoft Reader) do not. *See* http://www.ebookmall.com/aboutebooks.htm (last visited Oct. 30, 2003). In the latter case, the use control apparently prevents the reader from exercising a public domain right.

95. 17 U.S.C. § 1201(b)(1)(A). *See* Lunney, Jr., *supra* note 21, at 842 ("Almost invariably, the same decryption technology that enables individuals to decrypt works not protected by copyright will also enable individuals to decrypt works protected by copyright.").

96. Some may argue that defendants have little to fear from criminal prosecution under the DMCA because the *Elcom* case, the only criminal DMCA anti-trafficking case to have been litigated, ended with an acquittal. Although one never knows exactly why a jury acquits a defendant, a reasonable explanation may be the judge's instruction to the jury that the defendant could not be guilty unless it knew that its product was illegal and intended to violate the law. Given that the defendant was a Russian company that removed its product from the Internet upon being notified of its illegality, it is entirely possible that the jury did not believe that the defendant had the relevant state of mind. *See* Lisa M. Bowman, *ElcomSoft Verdict: Not Guilty*, CNET NEWS.COM, Dec. 17, 2002, *at* http://news.com.com/2100-1023-978176.html (last visited Oct. 30, 2003) (reporting the acquittal of defendant ElcomSoft, its status as a Russian company, and the judge's instruction that guilt required actual knowledge of

Similar problems arise when a copyrighted work comes bundled with public domain material. Bundling happens all the time. History books contain copies of the Constitution and letters by historical figures that have passed into the public domain. Telephone books contain both copyrightable yellow pages and uncopyrightable white pages.[97] Law school casebooks combine the copyrightable commentary of authors with public domain cases.[98] If such works were to be distributed in digital form, then the publishers could implement DRM schemes that limit the uses a digital reader could make of these works. The DRM scheme might not allow any printing of the book, or it might not allow any copying of the book. It might even restrict the number of times a person can read the book.

These restrictions are arguably reasonable as to the copyrighted portions of the work. However, as to the public domain portions of the work, they are obviously unreasonable. Members of the public have unlimited rights of access to and use of public domain works, and it is entirely legal for consumers who already have legally obtained access to the copyrighted work to circumvent DRM to exercise those rights. Once again, however, the DMCA's anti-trafficking provisions make it virtually impossible for the public to get the technology needed to exercise its rights. To be sure, a person might in theory develop and market the necessary circumvention technology. That person, however, would also run a serious risk of civil or criminal prosecution because the technology in question would also allow users to make infringing uses of the copyrighted parts of the work. Such risks would understandably drive many potential developers of such technology into other lines of work.

Yet another example of this problem is the relationship of DRM to the limited duration of copyright. As noted earlier, the Constitution authorizes Congress to secure authors' copyright rights "for limited times."[99] The present copyright law follows this directive by capping

---

illegality and intent to violate the law) (on file with author). If the explanation offered here is correct, then the *Elcom* acquittal offers little comfort to potential defendants, at least American ones. Such a defendant would have a much harder time than ElcomSoft in convincing a jury that it did not know about laws against selling circumvention technology.

97. *See Feist*, 499 U.S. at 363 (holding white pages uncopyrightable); Bellsouth Adver. & Publ'g Corp. v. Donnelly Info. Publ'g, Inc., 933 F.2d 952, 958 (11th Cir. 1991) (holding plaintiff's yellow pages directory copyrightable).

98. Section 105 of the copyright code denies copyright to any work of the U.S. government. 17 U.S.C. § 105. Accordingly, opinions of federal courts are in the public domain. By contrast, the editorial comments of casebook authors are obviously copyrightable as works of authorship under § 102(a) of the code. *Id.* § 102(a) (defining copyrightable subject matter).

99. U.S. CONST. art. I, § 8, cl. 8.

the duration of copyright at seventy years after an author's death.[100] Thus, the works of an author who passes away in 2005 would pass into the public domain in 2075. Although it might seem unfair that a copyright holder's rights should suddenly disappear in the future, the U.S. Supreme Court has made it clear that such a result is the clear bargain of copyright law.[101] Authors get a monopoly that restricts public rights of access and use for a limited number of years. In exchange, the public gets free access and use after the term of copyright expires.

Unfortunately, digital protection for copyrighted works does not, and is not capable of, respecting the limited duration of copyright rights. Consider again a book written by an author who hypothetically will pass away in 2005. The publisher of that book could release a digital version in 2003 that is protected by DRM. That DRM gets the full protection of the DMCA's anti-trafficking provisions, so it is highly unlikely that any reader of the work will get the technology necessary to break the DRM scheme. When the book in question passes into the public domain in 2075, the public gains its free rights of access and use. However, the DRM scheme continues to operate at that time even though copyright rights have expired.[102] Thus, consumers would be within their rights to circumvent whatever aspect of the DRM they desired, but they would not have the technology to do so because its sale and development will have been outlawed for decades.

b. Anti-trafficking and Noninfringing Uses of Copyrighted Material

The problems associated with anti-trafficking and public domain material alone are meaningful. Even more problems arise when one also considers the effect of anti-trafficking on legal uses of copyrighted materials. Here too, problems exist because the DMCA's anti-trafficking provisions do not distinguish between DRM that protects a copyright holder's rights and DRM that tries to control rights that belong to the public.

The most obvious examples of this are the specifically enumerated instances where it is legal to circumvent DRM to gain access to a copyrighted work. As noted before, libraries can sometimes circumvent

---

100. 17 U.S.C. § 302 (setting a limited duration for copyright).

101. *See Sony*, 464 U.S. at 429 (stating that the copyright monopoly "is intended to motivate the creative activity of authors and inventors by the provision of a special reward, and to allow the public access to the products of their genius after the limited period of exclusive control has expired").

102. This happens because the copyright holder would have no way of knowing how long the author would live at the time DRM protected books are sold. Thus, even if the copyright holder were inclined to include automatic expiration as part of its DRM, she would not know when to have the expiration kick in.

DRM to determine whether they want to buy a work.[103] Individuals can sometimes circumvent when protecting their privacy, and when DRM has failed on account of malfunction, damage, or obsolescence.[104] These instances of circumvention are allowed because they do not lead to copyright infringement. The individuals who hold these rights of noninfringing circumvention need circumvention technology to exercise their rights.

The DMCA's anti-trafficking provisions, however, make no distinction between circumvention technology used for these purposes and circumvention technology used for infringing purposes, and the courts do not seem inclined to read such a distinction into the statute.[105] Again, those who want to buy technology to exercise these rights cannot do so because anyone selling the technology risks felony prosecution. The anti-trafficking provisions therefore impose an effective forfeiture of these rights.

A similar problem occurs when one studies circumvention of use-control DRM. As has already been noted, circumvention here is legal because the DMCA only prohibits circumvention for purposes of access.[106] Moreover, the circumvention need not be undertaken for purposes of committing infringement. Once again, however, the DMCA's anti-trafficking provisions make it practically impossible for a person to exercise her legal rights.

A DRM scheme that prohibits copying of a work provides an excellent example of the problems in question because it is precisely the type of DRM that would be imposed to defeat copyright infringement on the Internet. If users of a work cannot copy it, then there will be no infringing files to post on the Internet. Unfortunately, a digitally imposed prohibition against copying does a lot more than prevent infringement because the copyright code often allows individuals to make full or partial copies of a work.[107]

For example, the fair-use doctrine gives individuals the right to copy works when broadcast for television in order to view them at a more convenient time.[108] It is also fair use for someone to load a copy of a CD onto the hard disk of a computer for convenient listening, or to make a backup copy.[109] Fair use also allows people to reproduce small parts of a book in a book review, or include a short film clip in a

---

103. *See* 17 U.S.C. § 1201(d); *see also supra* text accompanying note 84.

104. *See* 17 U.S.C. §§ 1201(a)(1)(B)-(C), 1201(i); 37 C.F.R. § 201.40(b)(1)-(2); *see also supra* text accompanying notes 83, 85-86.

105. *See supra* note 77 and accompanying text.

106. *See supra* note 79 and accompanying text.

107. *See supra* notes 44-56 and accompanying text.

108. *See supra* note 53 and accompanying text.

109. *See supra* notes 49-50 and accompanying text.

lecture.[110] It also is fair use for teachers to make multiple copies of an article from the morning newspaper for contemporaneous or near-contemporaneous distribution to a class.[111] Other provisions of the copyright code permit copying as well.

A DRM scheme that prohibits copying of a work inhibits the exercise of every one of these rights. A person who wants to exercise these rights can legally circumvent such DRM as long as she already has legal access to the work. However, the anti-trafficking provisions make it illegal to sell the necessary technology to her because the same DRM that keeps her from exercising her rights also keeps her from committing copyright infringement.

3. EVALUATING THE DMCA'S ANTI-TRAFFICKING PROVISIONS

The foregoing shows that the DMCA's anti-trafficking provisions are a questionable solution to the problem of digital copyright infringement. The anti-trafficking provisions make it more difficult for individuals to commit copyright infringement. However, they also deprive individuals of technology needed to exercise legal rights of circumvention and noninfringing uses of copyrighted works.

A supporter of the DMCA would probably brush aside these problems by minimizing the importance of the losses caused by the anti-trafficking provisions. They might point out that those who desire access to public domain materials can often get them in a form unaffected by DRM. For example, most digital public-domain books exist in print, and older movies exist in VHS format. Even when a work is available only in digital form with DRM, a user who gains lawful access to the work can still make copies, whether by transcribing the work or taking a photograph of the relevant computer screen. Thus, the anti-trafficking provisions do not really impede access to public domain works and noninfringing uses. They simply remove the most convenient method for enjoying those rights, which is seemingly a small price to pay for the elimination of copyright infringement.[112] However, further analysis shows that we should not dismiss the public's convenience quite so easily.

The critical insight comes from realizing that DRM gives copyright holders an unprecedented degree of control over their works, control

---

110. *See supra* note 51 and accompanying text.

111. *See* 17 U.S.C. § 107; *see also Agreement on Guidelines for Classroom Copyrighting in Not-For-Profit Educational Institutions with Respect to Books and Periodicals*, H.R. REP. NO. 94-1476, at 68-70 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5681-83.

112. *See Corley*, 273 F.3d at 459 ("Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique or in the format of the original.").

that allows copyright holders to charge users for something that is supposed to be free. In a pre-digital world, those selling books, recorded music, and movies generally lost control of those works upon sale. Purchasers could read a book whenever and as often as they liked. They could photocopy limited portions of the work for personal use, lend the book to a friend, or even cut out the photographs from the book and resell them. Once a copy of a book left the seller's hands, any person who subsequently gained possession of the book could use the book in the same way as the original purchaser.

Today, a copyright holder selling a digital copy of a work has many more options because practically any restriction can be written into a work's DRM. A copyright holder can now restrict whether a particular person can read a work, limit the number of times a work is read, prohibit printing, and prohibit digital copying. Sale of a digital file therefore does not cause the same loss of control as does the sale of a printed book. Indeed, copyright holders can use that control to collect money from the purchaser of a book even after a sale is made. For example, copyright holders might sell a novel on a disk that permits only five readings of the work, restricts viewing of the work to a single computer, and prohibits printing or copying. A purchaser would then have to contact the seller and pay extra for "upgrades" that would allow more reading of the work, selling or lending the work to a friend for viewing on the friend's computer, taking a printed version of the novel to the beach, or copying a few paragraphs from the digital file into a paper she is writing.[113]

It does not take a lot of imagination to see how DRM like this could change copyright's balance. That balance includes many noninfringing uses of works that the public has taken for granted because no one could control those uses for works sold in a pre-DRM world. DRM, however, gives copyright holders the power to take control of those previously uncontrolled uses. This control allows people who implement DRM to charge others for those noninfringing uses, even though those uses should be free.

To be sure, people who find their digital uses stymied could try to find analog versions of the work unaffected by DRM. However, such efforts will often be costly or impractical. For example, one court has

---

113. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 128–29 (1999) (describing how DRM could enable content providers to charge for various uses, including ones not presently protected as rights under copyright); *see also* Cohen, *supra* note 13, at 1093–94 ("Unhappily for consumers, however, digital rights management regimes will enable information providers to appropriate far more protection against copying and distribution than intellectual property law now provides."); R. Anthony Reese, *The First Sale Doctrine in the Era of Digital Networks*, 44 B.C. L. REV. 577, 614 (2003) (analyzing the challenges posed by digital networks to the principles behind the first sale doctrine).

suggested that users who want to make fair use of DVDs point a video camera at the screen of a computer that plays the DVD.[114] Such an exercise requires the purchase of an appropriate camera and the effort of setting up the camera so that a serviceable image can be captured. The cost of finding alternatives to noninfringing uses controlled by DRM gives copyright holders room to charge users for the privilege of exercising rights they already have. So long as copyright holders charge less than the cost of alternative noninfringing uses, users will prefer to pay copyright holders for noninfringing digital uses because it is cheaper than finding an alternative. This pattern effectively ensures that copyright holders who use DRM will hold on to their ability to charge people for rights that the people supposedly already have.

To sum up, the DMCA's anti-trafficking provisions have a significant impact on the public's ability to access and use both copyrighted works and material from the public domain. Despite arguments to the contrary, it is unwise to shrug off the DMCA's effect as simply a matter of public convenience because the longstanding balance of copyright may be at stake. It is therefore appropriate to ask whether society is wise to exchange the losses imposed by the DMCA for the security of copyrights. Supporters of the DMCA would no doubt answer this question affirmatively. They would surely claim that Congress was correct in its judgment that any compromise on the availability of circumvention technology would lead to rampant copyright infringement.[115] They might recognize the burdens the anti-trafficking provisions place on noninfringing uses, but they would accept the burdens as necessary to slow copyright infringement.

Brief reflection reveals that the persuasiveness of the argument in support of the DMCA rests heavily on the factual claim that no compromise on the availability of circumvention technology is possible, and that copyright infringement will run amok if such technology is ever lawfully sold. Such rampant infringement might occur if circumvention technology becomes available as software over the Internet. If that happens, then millions of people could anonymously acquire technology that defeats DRM and use it with little fear of being detected. However, this Article takes the position that the doomsday scenario sketched here is not inevitable. As will be shown below, a study of federal gun control reveals a number of regulatory techniques that would preserve access to circumvention technology for lawful purposes while offering meaningful protections against the misuse of that technology.

---

114. *See Corley*, 273 F.3d at 459 (noting that fair use of a DVD can be made with an analog video camera and stating: "Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique or in the format of the original").

115. *See supra* note 22.

II. FEDERAL GUN CONTROL

The federal gun control law[116] and the DMCA's anti-trafficking provisions are both responses to the misuse of technology. Just as people misuse circumvention technology to commit copyright infringement, they also misuse guns to commit murder, assault, rape, robbery, and other forms of theft. In both cases, Congress has passed laws designed to keep dangerous technology away from people in an effort to eliminate misuse. Both laws also have encountered criticism from those concerned about their effect on law-abiding citizens who use the technology for lawful purposes.[117]

Federal gun control offers an interesting point of comparison to the DMCA because Americans take both sides of the gun control debate seriously. Those outraged by gun violence have plenty of numbers from which to draw support. According to Bureau of Justice Statistics, guns are used in about 500,000 violent crimes per year.[118] In 2000, people used guns to commit more than 10,000 murders.[119] Economic estimates of losses traceable to guns run as high as $100 billion per year.[120] Surely, it is argued, such losses justify the removal of guns from society. At the same time, those concerned about the lawful use of guns point to estimates of between 100,000 and 2.5 million instances of self-defense with guns per year and the value of recreational weapons use.[121] Critics of gun control believe that the benefit of these uses easily outweighs whatever losses society suffers because of gun availability.[122]

---

116. The principal gun control statute is 18 U.S.C. §§ 922-930. However, there are literally enough miscellaneous provisions regulating guns to fill a book. *See* ALAN KORWIN & MICHAEL P. ANTHONY, GUN LAWS OF AMERICA, EVERY FEDERAL GUN LAW ON THE BOOKS 5-6 (1995) (containing over 200 pages of federal laws concerning guns).

117. *See supra* note 21 (citing articles expressing concern about the DMCA's effect on lawful use of circumvention technology); *see also* THE GUN CONTROL DEBATE: A DOCUMENTARY HISTORY (Marjolijn Bijlefeld ed., 1997) (containing various documents expressing support and opposition to gun control); MyNRA, National Rifle Association, *at* http://www.nra.org (website of the National Rifle Association, an organization generally critical of gun control).

118. According to Bureau of Justice Statistics, 533,470 victims of serious violent crime faced a gun during 2000. *See* Bureau of Justice Statistics, U.S. Dep't of Justice, *Firearms and Crime Statistics*, *available at* http://www.ojp.usdoj.gov//bjs/guns.htm (last visited Oct. 30, 2003) (on file with author).

119. *Id.*

120. PHILIP J. COOK & JENS LUDWIG, GUN VIOLENCE, THE REAL COSTS vii (2000).

121. *Id.* at 37 (reporting varying estimates of self-defense with guns).

122. *See* JOHN R. LOTT, JR., MORE GUNS, LESS CRIME: UNDERSTANDING CRIME AND GUN-CONTROL LAWS 19-20 (1998) (contending that widespread ownership of guns reduces the incidence of crime). It should be mentioned here that Lott's book has been

Not surprisingly, those fervently convinced about the merits or demerits of gun control have enough evidence and political clout to keep either side from achieving a total deregulation of guns or a total ban on guns. The resulting political struggles have forced Congress to write and rewrite federal gun control statutes in an effort to strike a compromise that seems right to the American public.[123] Federal gun control law therefore provides a good illustration of how Congress can restrict the availability of technology while preserving access for lawful purposes.[124]

The compromises inherent in federal gun control law are apparent from the history and content of the relevant statutes. As a general rule, Congress has enacted gun control legislation in response to public outrage over highly publicized incidents of gun violence. Concern over the use of guns by organized crime in the 1920s spurred the first major pieces of federal gun control legislation in the 1930s.[125] The assassinations of President John F. Kennedy, Dr. Martin Luther King, Jr., and Senator Robert F. Kennedy helped rally public support for passage of the Gun Control Act of 1968.[126] Likewise, the attempted assassination of President Ronald Reagan paved the way for the so-called Brady Act in 1993.[127] A string of school shootings and other

---

criticized by a number of scholars who question the integrity of his work. *See* Ian Ayers & John J. Donahue, *Shooting Down the "More Guns Less Crime" Hypothesis*, 55 STAN. L. REV. 1193 (2003); Chris Mooney, *Double Barreled Double Standards*, *at* MOTHERJONES.COM, http://www.motherjones.com/news/feature/2003/42/23_590_01.html (last visited Oct. 30, 2003) (summarizing critiques of Lott and his work). Nevertheless, these critiques do not change the fact that Lott (and others) believe that the benefit of guns outweighs their costs.

123. *See infra* notes 125-28 and accompanying text for a brief description of important laws strengthening gun control. The major legislation moderating gun control was the Firearms Owners' Protection Act, Pub. L. No. 99-308, § 1, 100 Stat. 449 (1986) (amending 18 U.S.C. § 921). For an analysis of this law, see David T. Hardy, *The Firearm Owners' Protection Act: A Historical and Legal Perspective*, 17 CUMB. L. REV. 585, 589 (1987).

124. *See* Gun Control Act § 101; Firearms Owners' Protection Act § 1 (identifying the need for additional legislation to protect the ability of law-abiding citizens to acquire and use guns for lawful purposes).

125. The statutes were the National Firearms Act of 1934, Pub. L. No. 73-474, 48 Stat. 1236 (1934), and the Federal Firearms Act of 1938, Pub. L. No. 75-785, 52 Stat. 1250 (1938). For a brief history of major federal gun control legislation see GUN CONTROL: AN AMERICAN ISSUE 11-23 (Nancy R. Jacobs et al. eds. 1997) [hereinafter GUN CONTROL]; Hardy, *supra* note 123 at 589-95 (offering a history of major federal gun control legislation and noting that public violence motivated the enactment of many gun laws).

126. See Jacobs et al., *supra* note 125, at 12 (reporting the influence of assassinations on gun control legislation).

127. Pub. L. No. 103-159, 107 Stat. 1356 (1993) (amending 18 U.S.C. § 922). For a brief history of the Brady Handgun Violence Prevention Act, see GLENN H. UTTER, ENCYCLOPEDIA OF GUN CONTROL AND GUN RIGHTS 38-39 (2000).

tragedies galvanized support for bans against assault weapons in 1994,[128] and the ten killings committed by the Maryland snipers in 2002 may provide political impetus to legislation that would establish "ballistic fingerprinting" of all guns.[129]

Congress could have responded to all of this gun violence by enacting broad prohibitions against gun sale and ownership,[130] but it has chosen not to. Instead, Congress has explicitly stated that it wants to preserve access to weapons for lawful purposes,[131] and it has even deliberately relaxed federal gun laws perceived as unduly burdensome.[132] The result is a federal gun control statute that tries to keep guns from the hands of those most likely to misuse them.

The major statutory provisions that implement this scheme are presently found at 18 U.S.C. §§ 922–930. Although a detailed

---

128. Public Safety and Recreational Firearms Use Protection Act, Pub. L. No. 103-322, § 110102, 108 Stat. 1997 (1994) (amending 18 U.S.C. § 922).

129. *See* Press Release, Sen. Dianne Feinstein, Kohl, Feinstein Ballistics Bill Combats Gun Violence with Technology (Mar. 29, 2000) (describing introduction of federal ballistic fingerprinting legislation), *at* http://feinstein.senate.gov/releases00/ blast.html (last visited Sept. 5, 2003); Stephen P. Halbrook, *Post-Sniper Policy*, NAT'L L.J., Nov. 11, 2002, at A17 (analyzing merits of ballistic fingerprinting and noting claim that ballistic fingerprinting might have aided in apprehending the Maryland snipers more quickly).

130. Some readers may wonder why Congress has the power to enact gun control legislation at all given the Second Amendment's guarantee of "the right of the people to keep and bear Arms." U.S. CONST. amend. II. Although the Second Amendment could be interpreted to make gun control impossible, the Supreme Court has never done so. Instead, the Court has interpreted the Second Amendment as a guarantee relating to the maintenance of militias for the common defense. *See* Lewis v. United States, 445 U.S. 55, 65–66 n.8 (1980) (stating in a footnote that federal legislation restricting the use of firearms is constitutional and does not affect constitutionally protected liberties); United States v. Miller, 307 U.S. 174, 183 (1939) (reversing lower court ruling that the National Firearms Act violated the Second Amendment). Accordingly, twentieth century courts have consistently held that the Second Amendment does not establish an individual right to bear arms. *See* Hickman v. Block, 81 F.3d 98, 101 (9th Cir. 1996) ("[T]he Second Amendment is a right held by the states, and does not protect the possession of a weapon by a private citizen."); Love v. Pepersack, 47 F.3d 120, 124 (4th Cir. 1995) ("[T]he lower federal courts have uniformly held that the Second Amendment preserves a collective, rather than individual, right."). It should be noted, however, that some academic commentary has expressed skepticism about this interpretation of the Second Amendment. *See* Sanford Levinson, *The Embarrassing Second Amendment*, 99 YALE L.J. 637, 642, 658–59 (1989) (expressing concern that the Second Amendment has not received the academic attention it deserves and suggesting that it can easily be interpreted to protect an individual's right to bear arms). Nevertheless, for the time being at least, Congress writes gun control legislation with little constitutional constraint, at least from the Second Amendment.

131. *See supra* note 33.

132. *See* Firearms Owners' Protection Act § 1, 100 Stat. at 449 (stating that it is not the intention to unduly burden law-abiding citizens); Hardy, *supra* note 123, at 627–80 (analyzing the Firearms Owners' Protection Act and describing how it loosened some of the restrictions found in the Gun Control Act of 1968).

summary of the entire statute is beyond the scope of this Article, seven major components are of particular interest.

1. *Licensing*: Federal law prohibits anyone from "engag[ing] in the business of importing, manufacturing, or dealing in firearams" without a federal license.[133] The term "engage in the business" means that some people—namely casual hobbyists or collectors—can sell guns without a license. However, a person who "devotes time, attention, and labor . . . with the principal objective of livelihood and profit" through the repeated sale of guns must get the necessary license.[134] Those desiring such a license can obtain one by filing an application with the Attorney General. This application includes a photograph and fingerprints of the applicant, as well as a license fee that varies by the type of weapons to be sold.[135]

2. *Record keeping*: The gun control statute requires all licensees to keep records of "importation, production, shipment, receipt, sale, or other disposition of firearms at his place of business."[136] The Attorney General has the authority to inspect these records upon issuance of a warrant, in the course of a criminal investigation, or for ensuring compliance with record keeping requirements.[137]

3. *Restrictions on the form of gun transactions:* Those not licensed by the federal government cannot sell, receive, give, or transport firearms across state lines, except for a few narrow exceptions.[138] A similar prohibition applies to sales by unlicensed individuals to nonresidents of the seller's state.[139] Licensees have a bit more freedom. They can make interstate sales of weapons to other licensees,[140] and they can sell rifles and shotguns to nonresidents in face-to-face transactions as long as the sale was legal under the laws of the dealer's state and the purchaser's state.[141] Mail-order sales by licensees are limited to cases in which the purchaser submits a sworn statement certifying legal age and containing the name of the principal law enforcement officer of the delivery address. The licensee must then forward a copy of the sworn statement and a description of the weapon sold to that officer by

---

133. 18 U.S.C. §§ 922(a)(1)(A), 923(a).

134. *Id.* § 921(21)(a).

135. *Id.* § 923(a), (c), *amended by* 18 U.S.C.S. § 923(a), (c) (Supp. 2003).

136. *Id.* § 923(g)(1)(A).

137. *Id.* § 923(g)(1)(A)-(B), *amended by* 18 U.S.C.S. § 923(g)(1)(A)-(B) (Supp. 2003).

138. *Id.* § 922(a)(5). The exceptions include firearms inherited by will or intestate succession and those purchased in a legally authorized face-to-face transaction.

139. *Id.*

140. *Id.* § 922(a)(1)-(2).

141. *Id.* § 922(b)(3).

certified mail and delay shipment of the weapon for at least seven days after acknowledgement of receipt.[142]

4. *Bans against certain weapons*: The statute prohibits the sale of machine guns, short-barreled shotguns, and short-barreled rifles, except as the Attorney General may specifically authorize.[143] The statute also makes it generally unlawful to manufacture, transfer, or possess semiautomatic assault weapons,[144] and to make or sell guns that cannot be detected by metal detectors and airport x-ray machines.[145]

5. *Prohibitions directed at certain classes of individuals*: Present law makes it illegal to sell guns to those under indictment for or convicted of a crime punishable by imprisonment of more than one year, fugitives from justice, unlawful users of certain drugs, and those "adjudicated as a mental defective or . . . committed to any mental institution,"[146] aliens illegally in the United States, those who have been dishonorably discharged from the Armed Forces, former U.S. citizens who renounced their citizenship, those subject to restraining orders in domestic violence cases, and individuals convicted of a misdemeanor domestic violence offense.[147] Licensees cannot sell firearms to those under eighteen, and they cannot sell rifles or shotguns to those under twenty-one.[148]

6. *Background checks and waiting periods*: Under the so-called "Brady Law,"[149] a federal licensee may not transfer a firearm to any nonlicensee who does not have a permit without positively identifying the recipient from a photographic identification and performing a specified background check through federally established system. If the system responds with a unique identification number for the transaction, then the sale may proceed. Otherwise, the transaction must be delayed for 3 business days. If the system notifies the seller that the transaction would violate the law within those three days, then the transfer must be abandoned. Otherwise, the sale may proceed.[150]

7. *Graduated penalties for violation of gun control laws and use of guns in commission of crime*: 18 U.S.C. § 924 offers a fairly complicated series of penalties for violating gun control laws. In general, "willful" violation of most provisions results in a fine, a prison

142. *Id.* § 922(c).
143. *Id.* § 922(b)(4), *amended by* 18 U.S.C.S. § 922(b)(4) (Supp. 2003).
144. *Id.* § 922(v).
145. *Id.* § 922(p).
146. *Id.* § 922(d)(4).
147. *Id.* § 922(d). In some cases, the Attorney General can restore the ability of such a person to buy a gun. *Id.* § 925(c), *amended by* 18 U.S.C.S. § 925(c) (Supp. 2003).
148. *Id.* § 922(b)(1).
149. Brady Handgun Violence Prevention Act § 101.
150. 18 U.S.C. § 922(t)(1), (3).

sentence of up to five years, or both.[151] "Knowing" violation of more serious provisions (e.g., selling to a fugitive from justice, dealing in stolen weapons, or purchasing of a firearm with the intent to commit a felony) carry fines or imprisonment of up to five and in some cases ten years, or both.[152] Selling a gun to someone in violation of the Brady Law carries a prison sentence of up to one year and a fine, or both.[153] Those who use a firearm to commit a crime of violence or drug trafficking crime face sentences of up to thirty years in prison, depending on the type of firearm used.[154] In some cases, second offenses carry the prospect of life in prison.[155] Finally, the statute provides for the seizure of weapons knowingly sold or transported in violation of the law.[156]

These seven provisions create a plausible scheme for keeping guns away from those most likely to misuse them while preserving access for lawful purposes. Four separate, but related, regulatory themes form the heart of this effort.

First, the provisions impose accountability on those who manufacture, distribute, and use guns. Licensing restricts the number of people who can make or sell guns by raising a barrier to entry. This increases the value of involvement in the gun business. The potential loss of a valuable business means that licensed gun makers and dealers have a lot to lose by violating federal law. Accordingly, they have good reason to obey restrictions on the distribution of guns and other requirements like recordkeeping. Recordkeeping in turn makes it easier for law enforcement to find those who commit crimes with weapons, as do proposals for centralized gun tracking like ballistic fingerprinting.[157] The increased likelihood of apprehension and prosecution acts as a deterrent to those purchasers of guns who might be inclined to misuse them. Significant criminal penalties add to this scheme of accountability.

Second, the law blocks channels of distribution that seem relatively likely to put otherwise lawful guns in the hands of irresponsible people. For example, those who want to commit crimes with guns obviously desire anonymity. When faced with the choice between entering a licensed dealership where positive identification is likely and buying a weapon through the mail, most such purchasers would prefer the mail.

---

151. *Id.* § 924(a)(1).
152. *Id.* § 924(a)(1)-(2).
153. *Id.* § 924(a)(5).
154. *Id.* § 924(c)(1).
155. *Id.* § 924(c)(1)(C)(ii).
156. *Id.* § 924(d)(1).
157. *See supra* note 129 (citing sources that describe ballistic fingerprinting).

Federal gun laws therefore restrict sales through the mail and transportation of guns across state lines.

Third, the gun control statute bans certain types of firearms because they have a high potential for tragic misuse. Semiautomatic assault weapons, sawed-off shotguns, and machine guns are very deadly weapons capable of killing many people in short order. At the same time, they are unlikely candidates for use in hunting or self-defense. Banning them makes sense because it will save lives while sacrificing a relatively small amount of lawful use. By contrast, other guns like hunting rifles and pistols are considered less threatening to public safety and are more likely to be used for lawful purposes. The statute therefore permits sale of these weapons while taking steps to ensure responsible distribution.

Fourth, the statute prevents sales of guns to certain individuals on the judgment that they are particularly likely to misuse them. Convicted felons, those subject to domestic violence restraining orders, fugitives from justice, and minors all present greater risks of irresponsible gun ownership than the ordinary adult citizen. Refusing to sell guns to them is simply common sense.

The foregoing description of federal gun control law sets the stage for a critique of the DMCA's anti-trafficking provisions and the prevailing wisdom that no compromise over circumvention technology is possible. The federal gun control statute shows that Congress is entirely capable of drafting statutes that curtail the availability and misuse of technology while preserving access for lawful purposes. This does not mean that federal gun control law is perfect. Some undoubtedly feel that federal gun control unduly burdens lawful uses of firearms, while others argue that more should be done to restrict the flow of guns and increase accountability for misuse. Nevertheless, many of the regulatory techniques used in federal gun control are applicable to the problem of copyright infringement and circumvention technology, and it is to this subject that the Article now turns.

III. CIRCUMVENTION TECHNOLOGY CONTROL PATTERNED AFTER GUN CONTROL

The best way to see how federal gun control can inform the understanding of the DMCA is to consider how a circumvention control statute could be patterned on the ideas behind federal gun control. Such a statute would not ban the sale of circumvention technology. Instead, it would allow the sale of such technology subject to restrictions designed to impose accountability, restrict distribution of technology through unreliable channels, eliminate the forms of circumvention technology

most subject to misuse, and prohibit purchase of such technology by those likely to misuse it.

A. Accountability in the Manufacture and Distribution of Circumvention Technology

A circumvention technology control statute patterned after gun control law would start with the imposition of licensing and recordkeeping requirements for those who manufacture and distribute circumvention technology. As in gun control, such measures would give people the incentive to make and sell circumvention technology responsibly. A federal agency—perhaps the Department of Justice or Register of Copyrights—could issue licenses to those who want to make, sell, or distribute circumvention technology. The only exception to the licensing requirement would be those engaged in encryption research. These individuals would be free to share circumvention technology with each other as they presently do under a specific exemption from the DMCA's anti-trafficking provisions.[158]

Issuance of the license would depend on the applicant's demonstrating his or her responsibility. This might include a background free of adverse civil or criminal judgments involving trafficking in circumvention technology and a clean criminal record. Prospective licensees would also have to be positively identified and give the address and telephone number of the location where the business would be located. Similar requirements would apply to the relevant officers or other responsible parties of corporations and other business entities applying for licenses. Establishment of a licensing scheme would allow imposition of a recordkeeping system maintained by licensees, who would positively identify each purchaser of circumvention technology, make sure the person is eligible to buy circumvention technology, and record the purchaser's name, address, and telephone number.

This scheme of accountability could be backed up with graduated penalties for irresponsible distribution and misuse of circumvention technology. Licensees who sell circumvention technology in unauthorized ways would face fines and loss of their licenses. Those who sell such technology with specific knowledge that the purchaser intends to use it for purposes of infringement would face larger fines and possible prison terms. Finally, those who purchase or use circumvention technology to commit significant acts of infringement

158. *See* 17 U.S.C. § 1201(g) (exempting encryption research and encryption researchers from provisions concerning circumvention and distribution of circumvention technology).

(e.g., posting of multiple copies of works on the Internet) would also face fines and possible prison sentences.

B. Controlling the Form and Distribution of Circumvention Technology

Like gun control, circumvention technology control could operate by preventing the sale of such technology through certain channels that are likely to place technology in irresponsible hands. Circumvention technology poses its greatest threat to copyright when it is distributed as software over the Internet. In that context, a single piece of circumvention software can be distributed to numerous people who can use it anonymously. Those specifically interested in committing copyright infringement are particularly likely to take advantage of such anonymous distribution because it is highly unlikely that their misuse of circumvention technology will ever be traced back to them. Indeed, it is precisely this scenario that made initial distribution of DeCSS (the software that circumvents CSS) so threatening to the film industry.

Brief reflection reveals that Internet distribution of circumvention technology in software form has four separate risks: anonymity of distribution; anonymity of use; rapid multiplication of circumvention software; and uncontrolled distribution to those most interested in committing copyright infringement. Legal regulation of the form and distribution of circumvention technology could, however, significantly address these risks without resorting to the ban presently found in the DMCA's anti-trafficking provisions.

The necessary law would have three components. First, it would allow circumvention technology implementation only in the form of hardware.[159] Second, all such circumvention devices would have to be identified by a unique serial number that would be added as a digital fingerprint or watermark to any decrypted file created by the device. Third, the law would limit the sale of circumvention devices to face-to-face transactions involving a licensed dealer who would identify the purchaser and record her identity along with the serial number of the purchased device.

Together, these provisions would significantly reduce the likelihood of irresponsible use. As an initial matter, restricting circumvention technology to hardware implementation removes the possibility of rapid multiplication and distribution over the Internet. A person who acquires circumvention hardware cannot post it on the Internet. Instead, the person only possesses a single device that is difficult to copy.[160]

---

159. The exception for encryption research would, of course, also exist here.

160. In theory, a person might be able to reverse engineer a piece of hardware and either build a duplicate or write software performing the same function, but such an

Additionally, the use of serial numbers and digital fingerprints or watermarks significantly reduces the likelihood of anonymous use. A person who buys circumvention hardware must have her name recorded by the dealer who sells the device. If she uses the device to decrypt copyrighted files and posts them to the Internet, then the files can be traced back to her. Moreover, it will be very difficult for her to remove the serial number by tampering with her circumvention device because it is hardware, and not software. Software is relatively easy to reverse engineer and alter by adding new computer code. Hardware is more difficult to tamper with because changes made to a physical device are likely to result in damage that permanently destroys its function. At the very least, a person intent on using circumvention hardware for purposes of infringement would have to put forth considerable effort and expense to regain her anonymity.

Finally, forcing purchasers of circumvention hardware to visit a licensed dealer deters those most likely to misuse technology from acquiring it. Legitimate users, like legitimate gun owners, are probably willing to give up their personal information. However, irresponsible users will be reluctant to have their identities recorded and associated with the serial numbers on their devices because it is hard to use circumvention hardware in truly anonymous fashion. Requiring purchasers to visit licensed dealers further lowers the possibility of identity fraud that might be associated with other forms of sale, such as by mail, telephone, or the Internet.

C. Prohibiting Certain Individuals from Buying Circumvention Technology

Parallels can also be drawn between prohibiting the sale of guns to certain people and the possible prohibitions against the sale of circumvention technology to others. As noted earlier, federal gun control associates certain groups with a higher risk of gun misuse and explicitly bans gun sales to them. It is possible to do likewise with respect to circumvention technology, although perhaps on a more limited basis.

For example, it may be the case that those under twenty-one are more likely to misuse circumvention technology than older individuals. There are several possible reasons for this. First, young people may have more difficulty understanding copyright law than older individuals. Second, they may have access to broadband networks, particularly at colleges and universities, that make sharing of infringing files

---

effort would be sufficiently difficult to accomplish so that it is a meaningful impediment to someone who is trying to facilitate copyright infringement.

particularly attractive and easy. Third, their economic resources may be more limited than those of older people. Fourth, young people may, as a group, be testing the limits of authority. In any event, if Congress believes that those under twenty-one represent a particular risk, then it could prohibit the sale of circumvention technology to them. Licensed dealers could easily enforce this restriction by insisting on proof of age at the time of purchase. Of course, this does not mean that those under twenty-one would never get circumvention technology. A responsible adult could buy it for them and supervise its use.

Similarly, Congress could make the judgment that people who have been convicted of felonies, or perhaps only criminal copyright violations, have already demonstrated sufficient disregard for the law to justify a prohibition against the sale of circumvention technology to them. Such a proposal would, however, be more difficult to enforce than a prohibition against the sale of circumvention technology to those under twenty-one because no easy way of conducting background checks is available. To be sure, a declaration under penalty of perjury might suffice, but this would certainly be far from foolproof. Of course, it is theoretically possible to create a database with information about those who have been convicted of crimes or copyright violations, but in candor it is probably not worth the expense of doing so because copyright infringement is a less serious criminal offense than gun violence.

IV. ENGAGING THE PREVAILING WISDOM

The circumvention technology control law proposed above is not perfect. Many details need to be worked out, and changes may be desirable to strengthen or weaken particular provisions. Nevertheless, the proposal is advanced now because it shows how the law can protect the security of copyright while preserving public rights of access and use. This realization is important because, as noted earlier, the prevailing wisdom in Congress precludes the possibility of such a compromise.[161]

It is, of course, foolish to imagine that this Article's proposal will immediately change the minds of those who subscribe to the prevailing wisdom that the DMCA must ban circumvention technology.[162] At least

161. *See supra* notes 22–23 and accompanying text.

162. There will, of course, also be those who object the proposal made here because it does not eliminate the DMCA's anti-trafficking provisions. Although there is something to be said on behalf of such elimination, this Article chooses not to consider it for two reasons. First, the Article accepts the notion that copyright holders should have some amount of protection from copyright infringement, and that DRM can play a constructive role in protecting copyright rights. Second, it is completely unrealistic to think that Congress will repeal the DMCA anytime soon. Proposals that modify the

two possible objections can be anticipated. First, supporters of the DMCA will argue that the proposal unacceptably damages the security of copyright. Second, some may contend that the proposal is unnecessary because copyright holders are highly unlikely to impose DRM that deprives the public of desired uses. Each of these objections is worth exploring. Analysis shows, however, that the proposal is in fact wise policy. Instead of harming the security of copyright, the proposal encourages development of a legal market for circumvention technology that can be regulated to reduce misuse. Moreover, this market will encourage the development and implementation of reasonable DRM.

A. The Security of Copyright

It is easy to see why supporters of the DMCA would worry about the effect of this Article's proposal on the security of copyright. After all, the DMCA legislates a world in which ordinary people cannot commit copyright infringement against works protected by DRM because ordinary people cannot get the necessary technology. This Article's proposal gives people access to circumvention technology, thereby turning every member of the public into a potential infringer. This elevated risk of copyright infringement may be unacceptable to some, especially when compared with the perfect security called for under the DMCA. Careful analysis, however, shows that this argument carries more rhetorical heat than persuasive insight.

First, no law—not even a complete ban on circumvention technology—can guarantee the security of copyright. Piracy has always existed, yet copyright-based industries have flourished. It is therefore abundantly clear that perfect security is neither possible nor necessary to ensure the production of creative works.

Second, the proposal advanced here creates at most a marginal increase in the threat to copyright when compared to the existing DMCA regime. This realization follows from the observation that the DMCA's anti-trafficking provisions do not actually provide good security against circumvention technology. For example, the *Reimerdes* and *Corley* cases made it illegal to distribute DeCSS,[163] yet DeCSS remains freely available over the Internet.[164] This widespread availability shows that

---

DMCA stand a better chance of adoption, so it makes sense to concentrate the Article's efforts along those lines.

163. In *Reimerdes*, the defendants were enjoined from posting DeCSS for downloading from their website or knowingly linking to another web site where DeCSS was posted. *Reimerdes*, 111 F. Supp. 2d at 346–47 (final order of the court). In *Corley*, the Second Circuit upheld the lower court's order. *Corley*, 273 F.3d at 434–35.

164. A search of "DeCSS" using Google returned over 100,000 sites, many of which purported to have the software available for downloading. *See Where Can You*

people truly intent on distributing circumvention technology over the Internet will probably succeed, and people who really want circumvention technology will be able to get it from those willing to flout the law.[165] To put it a bit differently, the DMCA does not eliminate circumvention technology. Instead, it drives the market for such technology underground where the providers and users of the technology will support each other's efforts to remain anonymous and beyond the reach of the law.

By contrast, this Article's proposal permits development of a legal market for circumvention technology that can be regulated. People who want circumvention technology for lawful purposes have significant

---

Find DeCSS?, Harvard Law School Berkman Center for Internet & Society, *at* http://cyber.law.harvard.edu/openlaw/DVD/DeCSS/ (last visited Oct. 7, 2003) (providing information about how to obtain DeCSS).

165. Stopping the distribution of circumvention software over the Internet is a bit like trying to stop the distribution of child pornography over the Internet. Federal law prohibits individuals from using computers to transmit photographs of actual minors engaged in explicit sexual conduct. *See* 18 U.S.C. § 2252(a)(1). The Supreme Court has held that such a prohibition does not violate the First Amendment because the government has a particularly strong interest in protecting children from exploitation. *See* Aschroft v. Free Speech Coalition, 535 U.S. 234, 250–51 (2002) (explaining why the First Amendment does not protect photographs of actual minors engaged in explicit sexual behavior); New York v. Ferber, 458 U.S. 747, 763–65 (1982) (holding that the First Amendment does not protect child pornography). Accordingly, the federal government actively investigates and prosecutes cases of child pornography, including cases that involve distribution over the Internet.

The resources devoted to this effort are significant. At the federal level alone, the FBI reports that twenty-three task forces in fifty-six field offices devote all of their resources to the eradication of child pornography. Since 1995, this task force has initiated over 5,700 investigations that resulted in the arrest and conviction of over 3,000 persons. *See* Press Release, Federal Bureau of Investigation, Operation Candyman, (Mar. 18, 2002), *at* http://www.fbi.gov/pressrel/pressrel02/cm031802.htm (last visited Oct. 30, 2003). State and local law enforcement undoubtedly augment these efforts. Despite this considerable expenditure of resources, child pornography remains available over the Internet. *See* PHILIP JENKINS, BEYOND TOLERANCE: CHILD PORNOGRAPHY ON THE INTERNET (2001) (discussing the business of online child pornography and the availability of illegal images online); Philip Jenkins, *Bringing the Loathsome to Light*, THE CHRON. OF HIGHER EDUC., Mar. 1, 2002, at B16 (discussing the availability of child pornography on the Internet). This availability shows that child pornography laws can slow down, but not eliminate, the distribution of child pornography on the Internet.

The DMCA's anti-trafficking provisions suffer from the same problem. Banning the sale of circumvention technology may slow down the distribution of such technology, but it does not stop it. If the work of twenty-three task forces and the conviction of over 3,000 people are not enough to stop the distribution of child pornography, there is reason to believe that a similarly large law enforcement effort would not stop the Internet distribution of circumvention technology. Even if such a large effort could stop the distribution of circumvention technology, one has to wonder whether copyright infringement is as serious a social problem as the exploitation of children, and whether such a significant expenditure of resources is wise in the context of the DMCA.

reasons to buy it legitimately instead of downloading it from an unknown source over the Internet. A person who downloads illegal software from an unknown source exposes himself to a number of significant risks. Malicious pranksters could use files labeled as circumvention software to infect computers with viruses or to install other objectionable software. Downloaded software might prove incompatible with a particular user's hardware or software configuration, or it might not work as advertised. Moreover, it is highly unlikely that those who distribute illegal software will offer any technical support or service to users who encounter problems. Indeed, the distributor will probably be hard to find because he is hiding from the law.

Conversely, a person who buys legal hardware from a legitimate source will get a product that has been tested to work as advertised. The likelihood of viruses or other malicious pranks is very low. If problems arise, then technical support from either the manufacturer or retailer will likely be available. Finally, the purchaser has the full range of consumer remedies at his disposal if the manufacturer or retailer fails to stand behind the product.[166]

The risks of misuse associated with a legal market for circumvention technology differ significantly from the risks associated with an illegal market. Illegal markets create high risks of misuse because the anonymity associated with illegality shields the behavior of those prone to misuse. Accordingly, one must conclude that the DMCA allows, however unintentionally, the creation of an illegal market for circumvention technology that significantly threatens every DRM scheme that copyright holders are likely to try. By contrast, legal markets of the sort identified here create lower risks of misuse because appropriate legal regulation discourages those who might misuse circumvention technology.[167] The legal market created by this Article's proposal therefore adds relatively little to the risk of copyright infringement. Indeed, the primary risk of copyright infringement has

---

166. An example of this is the appearance and growth of companies that sell Linux operating system software. Linux is a free operating system that is developed cooperatively by many people around the world under the GNU General Public License, which guarantees the free copying, modification, and distribution of Linux. *See GNUGeneral Public License* (June 1991), *at* Linux Online!, http://www.linux.org/info/gnu.html (last visited Oct. 30, 2003). Most versions of Linux may be freely downloaded from the Internet. *See Some Facts About Downloading Linux*, *at* Linux Online!, http://www.linux.org/dist/download_info.html (last visited Oct. 30, 2003) (on file with author). Nevertheless, companies like Red Hat successfully offer versions of Linux for sale precisely because customers value the product testing and technical support. *See What Is Red Hat's Business Model?*, *at* Red Hat, http://www.redhat.com/about/mission/business_model.html (last visited Oct. 30, 2003).

167. *See supra* Part III.

come, and will continue to come, from the unregulated distribution of illegal circumvention software over the Internet. That market is illegal under the DMCA and remains so under this Article's proposal. Regrettably, little can be done to eliminate the illegal market without resorting to measures that are probably more expensive and intrusive than justified. It is therefore hard to see how this Article's proposal will significantly compromise the security of copyright because the primary threat to copyright is outlawed, but not eliminated, by both the DMCA and the proposal made here.

B. Encouraging the Use and Development of Reasonable DRM

The foregoing shows that this Article's proposal does not require a stark choice between a ban on circumvention technology and the security of copyright. Instead, the proposal raises a more nuanced cost-benefit analysis that actually comes out in favor of permitting limited, legal distribution of circumvention technology. The starting point for this analysis is the effect of this new market on the development and use of DRM.

As has already been noted, a major drawback of the DMCA's anti-trafficking provisions is its support for overreaching DRM schemes. Copyright holders will successfully charge the public for uses that should be free because the public will not have access to technology that allows circumvention of the relevant DRM. Supporters of the DMCA sometimes respond to this concern by arguing that copyright holders are highly unlikely to impose overreaching DRM. The argument starts with the observation that copyright holders impose DRM to maximize revenue. Maximization of revenue depends on sales to consumers. If consumers want something, then copyright holders will supply it to them for a price. Thus, if consumers really care about noninfringing uses, then copyright holders will respond with appropriately designed DRM.[168] The DMCA therefore imposes few, if any, losses on society because copyright holders will probably use DRM schemes that allow noninfringing uses. Accordingly, no reason exists for amending the DMCA's anti-trafficking provisions. This argument is certainly plausible, but there are at least two reasons to reject it as a complete answer to the problem of overreaching DRM.

First, there is no particular reason to assume that copyright holders will provide consumers with something simply because it is economically rational to do so. Economic theory may predict that all

168. *See* Kevin Featherly, *Consumers Will Keep Copyright Guards in Check*, NEWSBYTES, Aug. 29, 2001, *available at* LEXIS (reporting the argument that consumer demand will prevent imposition of overreaching DRM).

people are rational profit-maximizers,[169] but experience shows that people do not always act the way economic theory predicts.[170] Even if copyright holders are behaving rationally, they may not satisfy consumer wants because they make errors in determining consumer preferences or assessing the risks associated with less restrictive DRM. Accordingly, society should not rely on copyright holders to permit noninfringing uses if society truly values those uses.[171]

Second, and perhaps more importantly, there is a significant risk that copyright holders will charge consumers an inappropriately high price for permission to exercise their rights of fair use and access to copyrighted works. This risk arises because the DMCA's anti-trafficking provisions give copyright holders a monopoly over any uses that can be controlled with DRM. Copyright holders are therefore free to charge monopoly prices for uses that are supposed be free, and many would almost certainly do so. This monopoly pricing would harm the public interest because monopolists restrict supplies to support higher monopoly prices.[172] The public would wind up paying more for fewer rights of fair use and access to copyrighted works.

The obvious solution to any problem involving monopolies is the introduction of competition. If copyright monopolists refuse to provide consumers with reasonable DRM at appropriate prices, then other competing actors can and should step in to fill the void. Such competition will deter copyright holders from charging monopoly prices for uses that are supposed to be free.

This Article's proposal offers a beneficial form of the desired competition. Legal access to circumvention technology means that sellers of such technology compete against copyright holders to provide access to encrypted works. Copyright holders can provide that access

---

169. *See* COOTER & ULEN, *supra* note 40, at 10–11 (describing economic actors as rational profit maximizers).

170. Besides common sense, a significant body of research supports this observation. *See* Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 74 N.Y.U. L. REV. 630 (1999) (describing systematic behavior different from rational profit maximization); Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV. 989, 1050–65 (1997) (reviewing reasons that economically desirable transactions sometimes do not occur and noting that intellectual property holders sometimes refuse to license rights even when it is economically rational for them to do so); Gregory Mitchell, *Taking Behavioralism Too Seriously? The Unwarranted Pessimism of the New Behavioral Analysis of Law*, 43 WM. & MARY L. REV. 1907, 1913–29 (2002) (describing recent use of research from psychology to question the assertion that people always behave as rational profit maximizers).

171. *See* Lunney, *supra* note 21, at 843–44 (explaining how DRM puts copyright holders in position of making decisions about the contours of appropriate use and raising the concern that copyright holders will make those decisions based on their own self-interest).

172. *See* COOTER & ULEN, *supra* note 40, at 38, 250.

by designing it into DRM. If they fail to do so, then providers of circumvention technology will take up the slack because the purchase of circumvention technology results in access to encrypted works.

To be sure, copyright holders may complain that competition from circumvention technology providers is unfair because the availability of circumvention technology exposes copyright holders to the risk of infringement with no compensation. However, further analysis shows that such competition does not force copyright holders to expose themselves as suggested.

The key is the limitation of circumvention technology to hardware implementations. As has already been noted, circumvention technology in the form of software could be distributed at no charge to others, thereby multiplying the risk of copyright infringement. However, hardware cannot be so distributed, and it is highly unlikely that hardware will be given away for free. This limits the risk of infringement associated with circumvention technology, and it guarantees that consumers who desire such technology will have to pay for it.

The cost of circumvention hardware also gives copyright holders fair protection against the perceived risk of competition from circumvention hardware. Copyright holders and providers of circumvention hardware may be in competition with each other, but copyright holders hold the upper hand. As an initial matter, copyright holders control the DRM in question, so they do not have to incur the expense of figuring out how to accomplish the desired circumvention. Additionally, copyright holders do not have to incur the costs of manufacturing hardware. They can simply build permitted uses into DRM schemes. Finally, and most importantly, copyright holders can cut off demand for circumvention hardware by responding to consumer desires at a competitive price.

Consumers are most likely to buy circumvention hardware when DRM prohibits basic noninfringing uses that consumers have always enjoyed. For example, purchasers of music CDs may want to load the files on their MP3 players. They will turn to circumvention hardware if the CDs they buy come with DRM that blocks such use. However, they have little reason to buy such technology if copyright holders allow their customers to make customary and appropriate use of the CDs. Accordingly, copyright holders can suppress the demand for circumvention hardware by providing desired consumer uses at a price lower than the price charged for circumvention hardware.

Even if copyright holders choose not to provide consumers with all desired uses, each provided use makes the purchase of circumvention hardware less attractive. This means that the suggested compromise does not force copyright holders to give customers what they want for

free. It simply introduces competition that sets a competitive ceiling on what copyright holders can charge for looser DRM. This in turn creates an incentive for the creation and implementation of reasonable DRM.

C. Comparing Costs and Benefits

The foregoing analysis allows a rough summation of the costs and benefits of this Article's proposal. The obvious cost of the proposal is the risk of putting circumvention technology into the hands of people who might engage in misuse. However, that risk is acceptable because the technology will be distributed in a way that imposes accountability and impresses upon users the importance of responsible use.

The benefits of the proposal come in three parts. First, legalizing distribution of circumvention technology for lawful purposes will shrink and isolate the illegal market. Each person who gets circumvention technology from a legal source is less likely to get similar technology from an illegal one. The result is that fewer people will wind up with truly dangerous forms of circumvention technology—namely those that operate anonymously—and this lowers the likelihood of copyright infringement. Second, and more importantly, the proposal restores public rights of access and use that the DMCA's anti-trafficking provisions seriously curtail. It is hard to quantify the value of these uses, but their value is likely to be significant because these public rights are closely associated with the maintenance of a copyright scheme that benefits society and respects constitutional boundaries.[173] Third, and perhaps most significantly, the proposal encourages the development and implementation of reasonable DRM schemes.

When these three benefits are added together, the sum appears to be larger than the marginal losses associated with the proposal's regulated distribution of circumvention hardware. The proposal is therefore wise policy.

V. CONCLUSION

This Article has described the DMCA's anti-trafficking provisions and the debate that surrounds them. It has used federal gun control law to show that society does not face an all-or-nothing choice between the total control of DRM and rampant copyright infringement. A circumvention technology control law modeled after federal gun control law will deter the irresponsible misuse of circumvention technology while preserving access to such technology for lawful purposes. Of

---

173. *See supra* Part I.A (describing the importance of public rights of access and use).

course, the proposal advanced here is not the only possible solution to the problems of copyright infringement and overreaching DRM, and many refinements to the ideas contained in the proposal will no doubt emerge as interested parties and policymakers consider it. Nevertheless, this Article has shown that retreat from the DMCA's hard-line stance against circumvention technology is wise policy. Hopefully, the ideas presented here will prove helpful as society continues its efforts to balance copyright incentives and the public's rights of access and use.