ELECTRONIC FRONTIER FOUNDATION

Unintended Consequences:

Ten Years under the DMCA

This document collects reported cases where the anti-circumvention provisions of the DMCA have been invoked not against pirates, but against consumers, scientists, and legitimate competitors. It will be updated from time to time as additional cases come to light. The latest version can always be obtained at www.eff.org.

1. Executive Summary

Since they were enacted in 1998, the "anti-circumvention" provisions of the Digital Millennium Copyright Act ("DMCA"), codified in section 1201 of the Copyright Act, have not been used as Congress envisioned. Congress meant to stop copyright infringers from defeating anti-piracy protections added to copyrighted works and to ban the "black box" devices intended for that purpose.[1]

In practice, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities, rather than to stop copyright infringement. As a result, the DMCA has developed into a serious threat to several important public policy priorities:

The DMCA Chills Free Expression and Scientific Research.

Experience with section 1201 demonstrates that it is being used to stifle free speech and scientific research. The lawsuit against *2600* magazine, threats against Princeton Professor Edward Felten's team of researchers, and prosecution of Russian programmer Dmitry Sklyarov have chilled the legitimate activities of journalists, publishers, scientists, students, programmers, and members of the public.

The DMCA Jeopardizes Fair Use.

By banning all acts of circumvention, and all technologies and tools that can be used for circumvention, the DMCA grants to copyright owners the power to unilaterally eliminate the public's fair use rights. Already, the movie industry's use of encryption on DVDs has curtailed consumers' ability to make legitimate, personal-use copies of movies they have purchased.

The DMCA Impedes Competition and Innovation.

Rather than focusing on pirates, some have wielded the DMCA to hinder legitimate competitors. For example, the DMCA has been used to block aftermarket competition in laser printer toner cartridges, garage door openers, and computer maintenance services. Similarly, Apple invoked the DMCA to chill RealNetworks' efforts to sell music downloads to iPod owners.

The DMCA Interferes with Computer Intrusion Laws.

Further, the DMCA has been misused as a general-purpose prohibition on computer network access, a task for which it was not designed and to which it is ill-suited. As a result, a disgruntled employer has used the DMCA against a former contractor for simply connecting to the company's computer system through a VPN.

2. DMCA Legislative Background

Congress enacted the DMCA's anti-circumvention provisions in response to two pressures. First, Congress was responding to the perceived need to implement obligations imposed on the U.S. by the 1996 World Intellectual Property Organization (WIPO) Copyright Treaty. Section 1201, however, went further than the WIPO treaty required.[2] The details of section 1201, then, were a response not just to U.S. treaty obligations, but also to the concerns of copyright owners that their works would be widely pirated in the networked digital world.[3]

Section 1201 contains two distinct prohibitions: a ban on ***acts*** of circumvention, and a ban on the ***distribution of tools and technologies*** used for circumvention.

The "act" prohibition, set out in section 1201(a)(1), prohibits the act of circumventing a technological measure used by copyright owners to control access to their works ("access controls"). So, for example, this provision makes it unlawful to defeat the encryption system used on DVD movies. This ban on acts of circumvention applies even where the purpose

for decrypting the movie would otherwise be legitimate. As a result, the motion picture industry maintains that it is unlawful to make a digital copy ("rip") of a DVD you own for playback on your iPod.

The "tools" prohibitions, set out in sections 1201(a)(2) and 1201(b), outlaw the manufacture, sale, distribution, or trafficking of tools and technologies that make circumvention possible. These provisions ban both technologies that defeat *access* controls, and also technologies that defeat use restrictions imposed by copyright owners, such as *copy controls*. These provisions prohibit the distribution of "DVD back-up" software, for example.

Section 1201 includes a number of exceptions for certain limited classes of activities, including security testing, reverse engineering of software, encryption research, and law enforcement. These exceptions have been extensively criticized as being too narrow to be of real use to the constituencies who they were intended to assist.[4]

A violation of any of the "act" or "tools" prohibitions is subject to significant civil and, in some circumstances, criminal penalties.

3. Chilling Free Expression and Scientific Research

Section 1201 has been used by a number of copyright owners to stifle free speech and legitimate scientific research.

The lawsuit against *2600* magazine, threats against Professor Edward Felten's team of researchers, and prosecution of the Russian programmer Dmitry Sklyarov are among the most widely known examples of the DMCA being used to chill speech and research. Bowing to DMCA liability fears, online service providers and bulletin board operators have censored discussions of copy-protection systems, programmers have removed computer security programs from their websites, and students, scientists and security experts have stopped publishing details of their research.

These developments will ultimately result in weakened security for all computer users (including, ironically, for copyright owners counting on technical measures to protect their works), as security researchers shy away from research that might run afoul of section 1201.

DMCA Delays Disclosure of Sony-BMG "Rootkit" Vulnerability

J. Alex Halderman, a graduate student at Princeton University, discovered the existence of several security vulnerabilities in the CD copy-protection software on dozens of Sony-BMG titles. He delayed publishing his discovery for several weeks while consulting with lawyers in order to avoid DMCA pitfalls. This left millions of music fans at risk longer than necessary.[5] The security flaws inherent in Sony-BMG's "rootkit" copy-protection software were subsequently publicized by another researcher who was apparently unaware of the legal risks created by the DMCA.

Security researchers had sought a DMCA exemption in 2003 in order to facilitate research on dangerous DRM systems like the Sony-BMG rootkit, but their request was denied by the U.S. Copyright Office.[6] In 2006, the Copyright Office granted an exemption to the DMCA for researchers examining the security threat posed by copy protection software on compact discs.[7] This exemption, however, does nothing to protect researchers studying other DRM systems.

Cyber-Security Czar Notes Chill on Research

Speaking at MIT in October 2002, White House Cyber Security Chief Richard Clarke called for DMCA reform, noting his concern that the DMCA had been used to chill legitimate computer security research. The *Boston Globe* quoted Clarke as saying, "I think a lot of people didn't realize that it would have this potential chilling effect on vulnerability research."[8]

Professor Felten's Research Team Threatened

In September 2000, a multi-industry group known as the Secure Digital Music Initiative (SDMI) issued a public challenge encouraging skilled technologists to try to defeat certain watermarking technologies intended to protect digital music. Princeton computer science professor Edward Felten and a team of researchers at Princeton, Rice, and Xerox took up the challenge and succeeded in removing the watermarks.

When the team tried to present their results at an academic conference, however, SDMI representatives threatened the researchers with liability under the DMCA. The threat letter was also delivered to the researchers' employers and the conference organizers. After extensive discussions with counsel, the researchers grudgingly withdrew their paper from the conference. The threat was ultimately withdrawn and a portion of the research was published at a subsequent conference, but only after the researchers filed a lawsuit.

After enduring this experience, at least one of the researchers involved has decided to forgo further research efforts in this field.[9]

SunnComm Threatens Grad Student

In October 2003, Princeton graduate student J. Alex Halderman was threatened with a DMCA lawsuit after publishing a report documenting weaknesses in a CD copy-protection technology developed by SunnComm. Halderman revealed that merely holding down the shift key on a Windows PC would render SunnComm's copy protection technology ineffective. Furious company executives then threatened legal action.

The company quickly retreated from its threats in the face of public outcry and negative press attention. Although Halderman was spared, the controversy again reminded security researchers of their vulnerability to DMCA threats for simply publishing the results of their research.[10]

Hewlett Packard Threatens SNOsoft

Hewlett-Packard resorted to DMCA threats when researchers published a security flaw in HP's Tru64 UNIX operating system. The researchers, a loosely-organized collective known as Secure Network Operations ("SNOsoft"), received the DMCA threat after releasing software in July 2002 that demonstrated vulnerabilities that HP had been aware of for some time, but had not bothered to fix.

After widespread press attention, HP ultimately withdrew the DMCA threat. Security researchers got the message, however—publish vulnerability research at your own risk.[11]

Blackboard Threatens Security Researchers

In April 2003, educational software company Blackboard Inc. used a DMCA threat to stop the presentation of research on security vulnerabilities in its products at the InterzOne II conference in Atlanta. Students Billy Hoffman and Virgil Griffith were scheduled to present their research on security flaws in the Blackboard ID card system used by university campus security systems but were blocked shortly before the talk by a cease-and-desist letter invoking the DMCA.

Blackboard obtained a temporary restraining order against the students and the conference organizers at a secret "ex parte" hearing the day before the conference began, giving the students and conference organizer no opportunity to appear in court or challenge the order before the scheduled presentation. Despite the rhetoric in its initial cease and desist letter, Blackboard's lawsuit did not mention the DMCA. The invocation in the original cease-and-desist letter, however, underscores the way the statute has been used to chill security research.[12]

Xbox Hack Book Dropped by Publisher

In 2003, U.S. publisher John Wiley & Sons dropped plans to publish a book by security researcher Andrew "Bunnie" Huang, citing DMCA liability concerns. Wiley had commissioned Huang to write a book that described the security flaws in the Microsoft Xbox game console, flaws Huang had discovered as part of his doctoral research at M.I.T.

Following Microsoft's legal action against a vendor of Xbox "mod chips" in early 2003, and the music industry's 2001 DMCA threats against Professor Felten's research team, Wiley dropped the book for fear that the book might be treated as a "circumvention device" under the DMCA. Huang's initial attempt to self-publish was thwarted after his online shopping cart provider also withdrew, citing DMCA concerns.

After several months of negotiations, Huang eventually self-published the book in mid-2003. After extensive legal consultations, Huang was able to get the book published by No Starch Press.[13]

Censorware Research Obstructed

Seth Finkelstein conducts research on "censorware" software (i.e., programs that block websites that contain objectionable material), documenting flaws in such software. Finkelstein's research, for example, revealed that censorware vendor N2H2 blocked a variety of legitimate websites, evidence that assisted the ACLU in challenging a law requiring the use web filtering software by federally-funded public libraries.[14]

N2H2 claimed that the DMCA should block researchers like Finkelstein from examining its software. Finkelstein was ultimately forced to seek a DMCA exemption from the Librarian of Congress, who granted the exemption in both the 2000 and 2003 triennial rulemakings. The exemption, however, was not renewed in 2006, leaving future researchers without protection from DMCA threats.[15]

Benjamin Edelman has also conducted extensive research into flaws in various censorware products. Edelman's research also led to evidence used by the ACLU in its constitutional challenge to the Children's Internet Protection Act (CIPA), which mandates the use of censorware by public libraries.

In the course of his work for the ACLU, Edelman discovered that the DMCA might interfere with his efforts to learn what websites are blocked by censorware products. Because he sought to create and distribute software tools to enable others to analyze the list if it changed, Edelman could not rely on the limited DMCA regulatory exception in place at the time. Unwilling to risk civil and criminal penalties under Section 1201, Edelman was forced to sue to seek clarification of his legal rights. Unfortunately, the court found that Edelman would have to undertake the research and hazard legal reprisals in order to have standing to challenge the DMCA. The case was therefore dismissed without addressing the DMCA's chill on research.[16]

Dmitry Sklyarov Arrested

In July 2001, Russian programmer Dmitry Sklyarov was jailed for several weeks and detained for five months in the United States after speaking at the DEFCON conference in Las Vegas.

Prosecutors, prompted by software goliath Adobe Systems Inc., alleged that Sklyarov had worked on a software program known as the Advanced e-Book Processor, which was distributed over the Internet by his Russian employer, ElcomSoft. The software allowed owners of Adobe electronic books ("e-books") to convert them from Adobe's e-Book format into PDF files, thereby removing restrictions embedded into the files by e-book publishers.

Sklyarov was never accused of infringing any copyright, nor of assisting anyone else to infringe copyrights. His alleged crime was working on a software tool with many legitimate uses, simply because other people *might* use the tool to copy an e-book without the publisher's permission.

Federal prosecutors ultimately permitted Sklyarov to return home, but brought criminal charges against ElcomSoft. In December 2002, a jury acquitted Elcomsoft of all charges, completing an 18-month ordeal for the wrongly-accused Russian software company.[17]

Scientists and Programmers Withhold Research

Following the Felten and Sklyarov incidents, a number of prominent computer security experts curtailed their legitimate research activities for fear of potential DMCA liability.

For example, when Dutch cryptographer and security systems analyst Niels Ferguson discovered a major security flaw in Intel's HDCP video encryption system, he declined to publish his results on his website on the grounds that he travels frequently to the U.S. and is fearful of "prosecution and/or liability under the U.S. DMCA law."[18]

Following the arrest of Dmitry Sklyarov, Fred Cohen, a professor of digital forensics and respected security consultant, removed his "Forensix" evidence-gathering software from his website, citing fear of potential DMCA liability. Another respected network security protection expert, Dug Song, also removed information from his website for the same reason. Mr. Song is the author of several security papers, including a paper describing a common vulnerability in many firewalls.[19]

In mid-2001 an anonymous programmer discovered a vulnerability in Microsoft's proprietary e-book DRM system, but refused to publish the results, citing DMCA liability concerns.[20]

Foreign Scientists Avoid U.S.

Foreign scientists have expressed concerns about traveling to the U.S. following the arrest of Russian programmer Dmitry Sklyarov. Some foreign scientists have advocated boycotting conferences held in the United States, and some conference organizers have decided to hold events in non-U.S. locations. In 2001, Russia went so far as to issue a travel advisory to Russian programmers traveling to the United States.[21]

Highly respected British Linux programmer Alan Cox resigned from the USENIX committee of the Advanced Computing Systems Association, the committee that organizes many of the U.S. computing conferences, because of concerns about traveling to the United States. He also urged USENIX to move its annual conference offshore.[22]

The International Information Hiding Workshop Conference, the conference at which Professor Felten's team intended to present its original SDMI watermarking paper, chose to break with tradition and held its next conference outside of the U.S. following the DMCA threat to Professor Felten and his team.[23]

IEEE Wrestles with DMCA

The Institute of Electrical and Electronics Engineers (IEEE), which publishes 30 per cent of all computer science journals worldwide, has also grappled with the uncertainties created by the DMCA. Apparently concerned about possible DMCA liability, the IEEE in November 2001 instituted a policy requiring all authors to indemnify IEEE for

any liabilities incurred should a submission result in legal action.

After an outcry from IEEE members, the organization ultimately revised its submission policies, removing mention of the DMCA. According to Bill Hagen, manager of IEEE Intellectual Property Rights, "The Digital Millennium Copyright Act has become a very sensitive subject among our authors. It's intended to protect digital content, but its application in some specific cases appears to have alienated large segments of the research community."[24]

2600 Magazine Censored

The *Universal City Studios* v. *Reimerdes* case illustrates the chilling effect that section 1201 has had on the freedom of the press.

In that case, eight major motion picture companies brought DMCA claims against *2600* Magazine seeking to block it from publishing DeCSS, a software program that defeats the CSS encryption used on DVD movies. *2600* had made the program available on its web site in the course of its ongoing coverage of the controversy surrounding the DMCA. The magazine was not involved in the development of software, nor was it accused of having used the software for any copyright infringement.

Notwithstanding the First Amendment's guarantee of a free press, the district court permanently barred *2600* from publishing, or even linking to, the DeCSS software code. In November 2001, the Second Circuit Court of Appeals upheld the lower court decision.[25]

In essence, the movie studios effectively obtained a "stop the presses" order banning the publication of truthful information by a news publication concerning a matter of public concern—an unprecedented curtailment of well-established First Amendment principles.[26]

CNET Reporter Feels Chill

CNET News reporter Declan McCullagh confronted the chilling effect of the DMCA firsthand. In the course of his reporting, he found four documents on the public website of the U.S. Transportation Security Administration (TSA). The website disclosed that the documents contained information about airport security procedures, the relationship between federal and local police, and a "liability information sheet." A note on the site stated that this "information is restricted to airport management and local law enforcement." The documents were distributed in encrypted form and a password was required to open and read them.

McCullagh obtained the passwords from an anonymous source, but did not open the documents, citing concerns that using a password without authorization might violate the DMCA.[27] This is particularly ironic, as any foreign journalist beyond the reach of the DMCA would be free to use the password.

"Journalists traditionally haven't worried about copyright law all that much," said McCullagh, "But nowadays intellectual property rights have gone too far, and arguably interfere with the newsgathering process."[28]

Microsoft Threatens Slashdot

In spring 2000, Microsoft invoked the DMCA against the Internet publication forum Slashdot, demanding that forum moderators delete materials relating to Microsoft's proprietary implementation of an open security standard known as Kerberos.

In the Slashdot forum, several individuals alleged that Microsoft had changed the open, non-proprietary Kerberos specification in order to prevent non-Microsoft servers from interacting with Windows 2000. Many speculated that this move was intended to force users to purchase Microsoft server software. Although Microsoft responded to this criticism by publishing its Kerberos specification, it conditioned access to the specification on agreement to a "click-wrap" license agreement that expressly forbade disclosure of the specification without Microsoft's prior consent.

Slashdot posters responded by republishing the Microsoft specification. Microsoft then invoked the DMCA, demanding that Slashdot remove the republished specifications.

In the words of Georgetown law professor Julie Cohen, "If Microsoft's interpretation of the DMCA's ban on circumvention technologies is right, then it doesn't seem to matter much whether posting unauthorized copies of the Microsoft Kerberos specification would be a fair use. A publisher can prohibit fair-use commentary simply by implementing access and disclosure restrictions that bind the entire public. Anyone who discloses the information, or even tells others how to get it, is a felon."[29]

GameSpy Menaces Security Researcher with DMCA

Luigi Auriemma, an independent Italian security researcher, attracted the attention of GameSpy's

lawyers after publishing details on his website regarding security vulnerabilities in GameSpy's online services, including a voice chat program, Roger Wilco, and online game finder, GameSpy 3D. Before publishing the information, Auriemma had informed GameSpy and public security mailing lists of the weaknesses. GameSpy, however, had failed to address the vulnerabilities.

In November 2003, GameSpy's lawyers sent a cease and desist letter to Auriemma, threatening civil and criminal penalties under the DMCA. According to GameSpy, Auriemma was publishing key generators and other piracy tools, rather than simply vulnerability research. Whatever the merits of GameSpy's claims, the invocation of the DMCA was likely improper in light of the fact that Auriemma resides in Italy and thus is beyond the reach of the DMCA.[30]

AVSforum.com Censors TiVo Discussion

The specter of DMCA litigation has chilled speech on smaller web bulletin boards, as well. In June 2001, for example, the administrator of AVSforum.com, a popular forum where TiVo digital video recorder owners discuss TiVo features, censored all discussion about a software program that allegedly permitted TiVo users to move video from their TiVos to their personal computers. In the words of the forum administrator, "My fear with this is more or less I have no clue what is a protected system on the TiVo box under copyright (or what-have-you) and what is not. Thus my fear for the site."[31]

Mac Forum Censors iTunes Music Store Discussion

Macintosh enthusiast website Macosxhints censored publication of information about methods for evading the copy protection on songs purchased from the Apple iTunes Music Store in May 2003, citing DMCA liability concerns. Songs purchased from the Apple iTunes Music Store are downloaded in Apple's proprietary AAC file format, wrapped in digital copy protection. As the webmaster for the site noted, even though information on bypassing the copy protection was readily available on the Internet at the time, republishing user hints on work-arounds risked attracting a DMCA lawsuit and harsh penalties.[32]

4. Fair Use Under Siege

"Fair use" is a crucial element in American copyright law—the principle that the public is entitled, without having to ask permission, to use copyrighted works in ways that do not unduly interfere with the copyright owner's market for a work. Fair uses include personal, noncommercial uses, such as using a VCR to record a television program for later viewing. Fair use also includes activities undertaken for purposes such as criticism, comment, news reporting, teaching, scholarship or research.

We are entering an era where books, music and movies will increasingly be "copy-protected" and otherwise restricted by technological means. Whether scholars, researchers, commentators and the public will continue to be able to make legitimate fair uses of these works will depend upon the availability of tools to bypass these digital locks.

The DMCA, however, prohibits the creation or distribution of these tools, even if they are crucial to fair use. So, as copyright owners use technology to press into the 21st century, the public will see fair uses whittled away by digital locks allegedly intended to "prevent piracy." Perhaps more importantly, **future fair uses will not be developed** for restricted media, because courts will never have the opportunity to rule on them. Fair users will be found liable for "picking the lock" and thereby violating the DMCA, whatever the merits of their fair use defense.

Copyright owners argue that these tools, in the hands of copyright infringers, can result in "Internet piracy." But banning the tools that enable fair use will punish the innocent along with infringers. Photocopiers, VCRs, and CD-R burners can also be misused, but no one would suggest that the public give them up simply because they might be used by others to break the law.

Although the Copyright Office is empowered to grant limited DMCA exemptions in a triennial rule-making, it has repeatedly refused to grant exemptions for consumer fair uses.[33]

Copy-protected CDs & DRM in Online Music

"Copy-protected" CDs and digital rights management (DRM) for online music illustrate the collision between fair use and the DMCA in the music world. As of early 2006, for instance, Sony-BMG had released more than 15 million copy-protected CDs in the U.S. market. Although the momentum toward universal CD copy-protection faltered after the Sony-BMG "rootkit" scandal in late-2005, no major label has publicly renounced the use of copy-protection on CDs.

Such CD copy-protection technologies interfere with the fair use expectations of music fans by

inhibiting the transfer of music from CD to iPods or other MP3 players—despite the fact that making an MP3 copy of a CD for personal use qualifies as a fair use. Other fair uses impaired by copy-protection technologies include making "mix CDs" or making copies of a CD for the office or car. Unfortunately, companies that distribute tools to "repair" these dysfunctional CDs, restoring to consumers their fair use privileges, run the risk of lawsuits under the DMCA's ban on circumvention tools and technologies.[34]

With the increasing popularity of online music, DRM has become an increasingly well-known frustration to fair use expectations for digital music, just as copy-protected CDs frustrated fair use expectations for physical CDs. Bypassing DRM to shift a song from one MP3 player to another, or to create a backup of the digital file, can expose a music fan to DMCA liability, even if all of the uses would otherwise qualify as non-infringing fair uses. Although more online music vendors are abandoning DRM—because, among other things, DRM has had no effect on piracy and, in the words of one digital content manager, eliminating DRM would solve "obvious interoperability issues"[35]—DRM is nevertheless another glaring example of the DMCA putting fair use under siege.[36]

Fair Use Tools Banned: DVD Software

Fair use of DVDs has suffered thanks to DMCA lawsuits brought against DVD copying tools. There are many legitimate reasons to copy DVDs. Once the video is on the PC, for example, lots of fair uses become possible—for example, video creators can remix movie clips into original YouTube videos, travelers can load the movie into their laptops, and DVD owners can skip the otherwise "unskippable" commercials that preface certain films. Without the tools necessary to copy DVDs, however, these fair uses become impossible.

In the *Universal v. Reimerdes* case, discussed above, the court held that the DMCA bans DeCSS software. In another case, federal courts ordered 321 Studios' DVD X Copy product taken off the shelves for violating the DMCA. Major movie studios also used the DMCA to sue Tritton Technologies, the manufacturer of DVD CopyWare, and three website distributors of similar software.[37]

Movie fans, film scholars, movie critics, and public interest groups have all repeatedly asked the Copyright Office to grant DMCA exemptions to allow the decryption of DVDs in order to enable noninfringing uses. For example, exemptions were sought to allow movie critics to post movie clips, DVD owners to skip "unskippable" previews and commercials, and legitimate purchasers to bypass "region coding" restrictions on their DVD players. Every DVD-related request was denied in both the 2000 and 2003 triennial rulemakings.[38] In 2006, a very narrow exemption was granted to allow media studies and film professors to create compilations of motion pictures for educational use in the classroom. The narrowness of this exemption was repeatedly emphasized by the Copyright Office: "If it had not been possible to define a class of works by reference to the users or the uses made of those works, it might have been difficult for the Register to recommend an exemption for this class of works."[39] This narrowness suggests future exemptions may only be granted if constraints can be placed on both the type of use *and* class of user—two heavy shackles on fair use.

Even if other narrow exemptions are granted in the future, it is worth noting that the Copyright Office is powerless to grant an exemption to the DMCA's "tools" ban. As a result, fair users are likely to be left with fewer tools at their disposal, even if they succeed in obtaining a DMCA exemption—few companies will want to enter a market making tools that could subject them to lawsuit.

Advanced e-Book Processor and e-Books

The future of fair use for books was at issue in the criminal prosecution of Dmitry Sklyarov and Elcomsoft. As discussed above, Elcomsoft produced and distributed a tool called the Advanced e-Book Processor, which translates e-books from Adobe's e-book format to PDF. This translation process removed various restrictions (against copying, printing, text-to-speech processing, etc.) that publishers can impose on e-books.[40]

The Advanced e-Book Processor allowed those who have legitimately purchased e-books to make fair uses of their e-books, uses otherwise made impossible by the restrictions of the Adobe e-book format. For instance, the program allowed people to engage in the following fair uses:

- read the e-book on a laptop or computer other than the one on which it was first downloaded;
- continue to access the e-book in the future, if the particular technological device for which it was purchased becomes obsolete;
- print an e-book on paper;

- read an e-book on an alternative operating system such as Linux (Adobe's format works only on Macs and Windows PCs);
- have a computer read an e-book out loud using text-to-speech software, which is particularly important for visually-impaired individuals.

Time-shifting and Streaming Media

As more people receive audio and video content from "streaming" Internet media sources, they will want tools to preserve their settled fair use expectations, including the ability to "time-shift" programming for later listening or viewing. As a result of the DMCA, however, the digital equivalents of VCRs and cassette decks for streaming media may never arrive.

Start-up software company Streambox developed exactly such a product, known simply as the Streambox VCR, designed to time-shift streaming media. When RealNetworks discovered that the Streambox VCR could time-shift streaming RealAudio webcasts, it invoked the DMCA and obtained an injunction against the Streambox VCR product.[41]

The DMCA has also been invoked to threaten the developer of an open source, noncommercial software application known as Streamripper that records MP3 audio streams for later listening.[42]

Agfa Monotype and Fonts

In January 2002, typeface vendor Agfa Monotype Corporation threatened a college student with DMCA liability for creating "embed," a free, open source, noncommercial software program designed to manipulate TrueType fonts.

According to the student: "I wrote embed in 1997, after discovering that all of my fonts disallowed embedding in documents. Since my fonts are free, this was silly—but I didn't want to take the time to… change the flag, and then reset all of the extended font properties with a separate program. What a bore! Instead, I wrote this program to convert all of my fonts at once. The program is very simple; it just requires setting a few bits to zero. Indeed, I noticed that other fonts that were licensed for unlimited distribution also disallowed embedding…. So, I put this program on the web in hopes that it would help other font developers as well."

Agfa Monotype nevertheless threatened the student author with DMCA liability for distributing the program. According to Agfa, the fact that embed can be used to allow distribution of protected fonts makes it contraband under Section 1201, notwithstanding the fact that the tool has many legitimate uses in the hands of hobbyist font developers.[43]

Agfa Monotype brought similar DMCA challenges against Adobe Systems for its Acrobat 5.0's FreeText Tool and Forms Tool, which allowed so-called "editable embedding." Agfa claimed that with Acrobat 5.0, the recipient of an electronic document could make use of embedded fonts to change the contents of a form field or free text annotation, thus "circumventing" the embedding bits of some of Agfa's TrueType Fonts.

Fortunately, in 2005, a federal court found that Adobe had not violated either Section 1201(a) or Section 1201(b) of the DMCA. The court noted that embedding bits do not effectively control access to a protected work and, moreover, that Acrobat 5.0 was not designed primarily to circumvent TrueType fonts.[44] Hopefully, this court ruling will discourage Agfa from making abusive DMCA threats in the future.

Load-'N-Go Space-shifting

In November 2006, movie studios wielded the DMCA to rein in Load-'N-Go, a small company that loaded DVDs purchased by a customer onto the customer's iPod. Load-'N-Go would take DVDs purchased by the customer, load the DVDs onto the customer's iPod, and then return both the iPod and the original DVDs.

The movie studios claimed this service violates the DMCA because creating a duplicate copy of the movie—even for personal, fair uses—circumvents the DVD's CSS encryption. Under this theory, any individual attempting to space-shift movies from DVD to iPod or to any other digital media player is violating the DMCA. Conveniently for movie studios, this legal posture enables them to sell consumers the same movies multiple times, for multiple devices.

After some back-and-forth in the courts, the case settled in February 2007.[45]

RealDVD Format-shifting

In October 2008, RealNetworks was forced to stop sales of its RealDVD software, designed to allow users to copy a DVD and store it on their hard drive. This format-shifting by RealDVD would empower consumers with numerous fair uses, such as allowing them to create backups, organize a movie collection

digitally, and watch a DVD at any time without being tied to a physical disc. These legitimate expectations of fair use were quickly stifled by a movie studio lawsuit, commenced the same day that RealDVD launched, alleging violations of the DMCA.

RealDVD makes an exact copy of everything on a DVD—including the DVD's CSS copy-protection system—and transfers it to the hard drive of a PC. A license from the DVD Copy Control Association authorizes RealNetworks to perform the necessary DVD decryption for this process. To ensure the resulting DVD copy cannot be shared or stolen, RealDVD encrypts the saved DVDs again and tethers the copy to a limited number of PCs.

Despite these layers of protection for copyrighted content and despite the numerous fair uses for which RealDVD was designed, a temporary restraining order was granted to halt the sale of RealDVD until a further hearing in late 2008.[46]

5. A threat to innovation and competition

The DMCA has frequently been used to deter legitimate innovation and competition, rather than to stop piracy.

For example, the DMCA has been used to block aftermarket competition in laser printer toner cartridges, garage door openers, and computer maintenance services. Apple Computer invoked the DMCA to chill Real Networks' efforts to sell music downloads to iPod owners. Videogame hobbyists have been sued for trying to improve or extend the capabilities of their favorite game titles. Sony has threatened hobbyists for creating software that enables Sony's Aibo robot dog to dance, and has sued to block software that allows gamers to play their PlayStation games on PCs.

In each of these cases, it was legitimate competitors and innovators who suffered, not pirates.[47]

DMCA Used First to Lock Cell Phones to Carriers; Then, to Hammer Phone Resellers

American cellular phone subscribers have long suffered with phones that are artificially "locked" to a particular carrier's network. This creates a variety of burdens for consumers, including high roaming rates when traveling (by preventing the use of prepaid SIM chips from local carriers) and barriers to switching carriers. In addition, these restrictions make locked phones harder to recycle and reuse. "Locking" phones seems particularly unjustifiable in light of the "minimum term" and "early termination fee" clauses that guarantee carriers will recoup the costs of the phones they are so fond of "giving away" to lure subscribers.

Responding to consumer demand, phone "unlocking" services have become widespread. Unfortunately, carriers responded by threatening legal action under the DMCA and, in at least one case, filing suit. Instead of being used against copyright infringers, the DMCA was used to prop up the anticompetitive business models of cellular carriers.[48]

At the 2006 triennial DMCA rulemaking, the Copyright Office granted an exemption for cell phone unlocking. Despite this exemption, however, DMCA lawsuits persist. Tracfone, the nation's largest independent prepaid-wireless provider, aggressively uses the DMCA to sue phone resellers who purchase and unlock Tracfone handsets. Courts have ruled in favor of Tracfone, allowing the company to continue using the DMCA as a hammer against secondary markets, instead of as a deterrent against copyright infringers.[49]

Apple Threatens Real over Harmony

In July 2004, RealNetworks announced its "Harmony" technology, which was designed to allow music sold by Real's digital download store to play on Apple iPods. Until Harmony, the only DRM-restricted music format playable on the iPod was Apple's own "Fairplay" format. Although the iPod plays a variety of DRM-free formats, Real wanted to ensure interoperability without having to give up DRM restrictions, and thus developed Harmony to "re-wrap" its songs using the Fairplay format.[50]

Within days, Apple responded by accusing Real of adopting the "tactics and ethics of a hacker" and threatening legal action under the DMCA. Over the following months, the two competitors engaged in a game of technological cat-and-mouse, with Apple disabling Harmony in updates of its iTunes software and Real revising its technology to re-enable compatibility. In the words of Real's filings before the SEC: "Although we believe our Harmony technology is legal, there is no assurance that a court would agree with our position."[51]

Tecmo Sues to Block Game Enhancements

Enthusiastic fans of the videogames Ninja Gaiden, Dead or Alive 3, and Dead or Alive Xtreme Beach Volleyball managed to modify their games to create new "skins" to change the appearance of characters who appear in the game (including making some characters appear nude). The modifications were add-

on enhancements for the games themselves—only those who already had the games could make use of the skins. These hobbyist tinkerers traded their modding tips and swapped skins on a website called ninjahacker.net.

Tecmo Inc., which distributes the games, was not amused and brought DMCA claims against the website operators and tinkerers who frequented it. The suit was ultimately dismissed after the website was taken down and settlements negotiated with the site's operators.[52]

Nikon's Encrypted RAW Format Blocks Adobe

In April 2005, the creator of Adobe's Photoshop revealed that camera-maker Nikon had begun encrypting certain portions of the RAW image files generated by its professional-grade digital cameras. As a result, these files would not be compatible with Photoshop or other similar software unless the developers first took licenses from Nikon. In other words, by encrypting the image files on its cameras, Nikon was obtaining market leverage in the image editing software market.

Adobe cited the prospect of a DMCA claim as one reason why it was unwilling to reverse engineer the format to facilitate interoperability. Nikon and Adobe ultimately negotiated an agreement, an option that may not be practical for smaller software developers in the future.[53]

HP's Region-Coded, Expiring Printer Cartridges

Hewlett-Packard, one of the world's leading printer manufacturers, has embedded software in its printers and accompanying toner cartridges to enforce "region coding" restrictions that prevent cartridges purchased in one region from operating with printers purchased in another. This "feature" presumably is intended to support regional market segmentation and price discrimination.

The software embedded in HP printer cartridges also apparently causes them to "expire" after a set amount of time, forcing consumers to purchase new ink, even if the cartridge has not run dry. This "feature" of HP ink cartridges has lead to at least one consumer class action against the company.

HP has not yet invoked the DMCA to protect these anti-consumer tactics, but both HP's lawyers and its competitors are doubtless well aware of ways in which the DMCA can be used to buttress these tactics.[54]

StorageTek Attempts to Block Independent Service Vendors

StorageTek sells data storage hardware to large enterprise clients. It also sells maintenance services for its products. Custom Hardware is an independent business that repairs StorageTek hardware. In an effort to eliminate this competitor in the maintenance services market, StorageTek sued under the DMCA, arguing that Custom Hardware had circumvented certain passwords designed to block independent service providers from using maintenance software included in the StorageTek hardware systems. In other words, StorageTek was using the DMCA to ensure that its customers had only one place to turn for repair services.

A district court granted a preliminary injunction against Custom Hardware. More than a year later, a court of appeals vacated the injunction, holding that where there is no nexus with copyright infringement, there can be no DMCA claim. Although this was a victory for competition, it illustrates the ways in which the DMCA continues to be used to impede competition, rather than prevent piracy.[55]

Lexmark Sues Over Toner Cartridges

Lexmark, the second-largest laser printer maker in the U.S., has long tried to eliminate the secondary market in refilled laser toner cartridges. In January 2003, Lexmark employed the DMCA as a new weapon in its arsenal.

Lexmark had added authentication routines between its printers and cartridges explicitly to hinder aftermarket toner vendors. Static Control Components (SCC) reverse-engineered these measures and sold "Smartek" chips that enabled refilled cartridges to work in Lexmark printers. Lexmark then used the DMCA to obtain an injunction banning SCC from selling its chips to cartridge remanufacturers.

SCC ultimately succeeded in getting the injunction overturned on appeal, but only after 19 months of expensive litigation while its product was held off the market. The litigation sent a chilling message to those in the secondary market for Lexmark cartridges.[56]

Chamberlain Sues Universal Garage Door Opener Manufacturer

Garage door opener manufacturer Chamberlain Group invoked the DMCA against competitor Skylink Technologies after several major U.S. retailers dropped Chamberlain's remote openers in favor of the less expensive Skylink universal

"clickers." Chamberlain claimed that Skylink had violated the DMCA because its clicker bypassed an "authentication regime" between the Chamberlain remote opener and the mounted garage door receiver unit. On Chamberlain's logic, consumers would be locked into a sole source not only for replacement garage door clickers, but virtually any remote control device.

Skylink ultimately defeated Chamberlain both at the district court and court of appeals, but only after many months of expensive litigation. In the words of the court of appeals, Chamberlain use of the DMCA was nothing less than an "attempt to leverage its sales into aftermarket monopolies."[57]

Sony Sues Connectix and Bleem

Sony has used DMCA to sue competitors who created emulation software that permits gamers to play PlayStation console games on PCs. In 1999, Sony sued Connectix, the maker of the Virtual Game Station, a PlayStation emulator for Macintosh computers. Sony also sued Bleem, the leading vendor of PlayStation emulator software for Windows PCs.

In both cases, Sony claimed that competitors had violated the DMCA by engaging in unlawful circumvention, even though the development of interoperable software has been recognized by the courts as a fair use under copyright law. Because courts have suggested that the DMCA trumps fair use, however, the DMCA has become a new legal weapon with which to threaten those who rely on reverse engineering to create competing products.

Neither Connectix nor Bleem were able to bear the high costs of litigation against Sony and pulled their products off the market. No similar emulation products have been introduced, effectively forcing gamers to use Sony console hardware if they want to play the PlayStation games they have purchased.[58]

Sony Threatens Aibo Hobbyist

Sony has also invoked the DMCA against a hobbyist who developed custom "dance moves" for his Aibo robotic "pet" dog. Developing these new routines for the Sony Aibo required reverse engineering the encryption surrounding the software that manipulates the robot. The hobbyist revealed neither the decrypted Sony software nor the code he used to defeat the encryption, but he freely distributed his new custom programs. Sony claimed that the act of circumventing the encryption surrounding the software in the Aibo violated the DMCA and demanded that the hobbyist remove his programs from his website.

Responding to public outcry, Sony ultimately permitted the hobbyist to repost some of his programs (on the understanding that Sony retained the right to commercially exploit the hobbyist's work). The incident illustrated Sony's willingness to invoke the DMCA in situations with no relationship to "piracy."[59]

Sony Attacks PlayStation "Mod Chips"

Sony has sued a number of manufacturers and distributors of "mod chips" for alleged circumvention under the DMCA. In doing so, Sony has been able to enforce a system of "region coding" that raises significant anticompetitive issues.

"Mod chips" are after-market accessories that modify Sony PlayStation game consoles to permit games legitimately purchased in one part of the world to be played on a games console from another geographical region. Sony complains that mod chips can also be used to play pirated copies of games. As noted above, it is hard to see why an independent vendor of a product with legitimate uses should have to solve Sony's piracy problems before entering the market.

Sony sued Gamemasters, distributor of the Game Enhancer peripheral device, which allowed owners of a U.S. PlayStation console to play games purchased in Japan and other countries. Although there was no infringement of Sony's copyright, the court granted an injunction under the DMCA's anti-circumvention provisions, effectively leaving gamers at the mercy of Sony's region coding system.

Interestingly, courts in Australia, recognizing the anticompetitive and anticonsumer potential of Sony's region coding system, came to a different conclusion under that country's analog to the DMCA. In *Stevens v Kabushiki Kaisha Sony Computer Entertainment*, the High Court of Australia held in 2005 that the regional access coding on Sony PlayStation computer games as implemented by the PlayStation console did not qualify for legal protection, as it did not prevent or inhibit copyright infringement.

Sony, like all vendors, is free to attempt to segregate geographic markets. If it does so, however, it should have to bear its own costs for the effort, rather than relying on the DMCA, which Congress plainly did not enact to trump the usual legal regimes governing parallel importation.[60]

Blizzard Sues bnetd.org

Vivendi-Universal's Blizzard Entertainment video game division brought a DMCA lawsuit against a

group of volunteer game enthusiasts who created software that allowed owners of Blizzard games to play their games over the Internet. The software, called "bnetd," allowed gamers to set up their own alternative to Blizzard's own Battle.net service.

Blizzard has a policy of locking in its customers who want to play their games over the Internet—it's the Battle.net servers or nothing. Although access to Blizzard's Battle.net servers is free, the hobbyists decided to create bnetd to overcome difficulties that they had experienced in attempting to use Battle.net. The bnetd software was freely distributed, open source, and noncommercial.

Blizzard filed suit in St. Louis to bar distribution of bnetd, alleging that the software was a "circumvention device" prohibited by the DMCA. According to Blizzard, the bnetd software could be used to permit networked play of pirated Blizzard games. The developers never used the software for that purpose, nor was that the purpose for which the software was designed.

It is hard to see why a competitor should have to solve Blizzard's piracy problem before it can offer innovative products for legitimate owners of Blizzard games. Nevertheless, Blizzard prevailed on its DMCA claim, and the bnetd developers ceased distributing the software.[61]

Apple Harasses Inventive Retailer

When Other World Computing (OWC), a small retailer specializing in Apple Macintosh computers, developed a software patch in 2002 that allowed all Mac owners to use Apple's iDVD software, they thought they were doing Macintosh fans a favor. For their trouble, they got a DMCA threat from Apple.

Apple's iDVD authoring software was designed to work on newer Macs that shipped with *internal* DVD recorders manufactured by Apple. OWC discovered that a minor software modification would allow iDVD to work with *external* DVD recorders, giving owners of older Macs an upgrade path. Apple claimed that this constituted a violation of the DMCA and requested that OWC stop this practice immediately. OWC obliged.

Rather than prevent copyright infringement, the DMCA empowered Apple to force consumers to buy new Mac computers instead of simply upgrading their older machines with an external DVD recorder.[62]

Macrovision Sues Sima for Digitizing Analog Signals

In April 2006, hardware manufacturer Sima Products was forced to stop selling various video enhancing products that digitized analog signals from DVD players and VCRs. Wielding the DMCA, Macrovision argued that Sima's analog-to-digital video enhancements circumvented Macrovision's analog copy protection (ACP).

Macrovision's ACP functions by inserting noise into the vertical blanking intervals found in analog video signals. This noise is not displayed on a television set, but it does degrade the recording made by most analog VCRs. Sima's products simply convert the analog signal into a digital signal, which eliminates additional noise in the blanking intervals, and then converts the signal back to analog. This video enhancement allows consumers to harness digital techniques to make up for a weakness in VCR analog technology, a weakness which could come from age or distortion as well as from techniques like Macrovision's.

ACP does not prevent digital copies. Moreover, when a digital copy is made, Macrovision's ACP does not survive. Accordingly, Sima's products are not "circumventing" anything by performing its analog-to-digital conversion.

Macrovision, nevertheless, was able to convince the court that Sima had violated the DMCA. This unfortunate result indicates that the DMCA can be manipulated to push obsolete analog copy protection systems onto new technology innovators.[63] Although Sima appealed the ruling, it subsequently settled with Macrovision before the appeal was heard.

Blizzard Attempts to Block World of Warcraft Glider

Blizzard, makers the popular online role-playing game World of Warcraft (WoW), sued MDY Industries, the developer of a program which enables WoW characters to continue playing even when the user is away from her computer. These "bot" programs help reduce the time that a user must otherwise spend to progress in the game. MDY's product, known as "Glider," proved to be very popular with WoW players, selling about 120,000 units.[64]

In July 2008, the court rejected several aspects of Blizzard's DMCA claim (leaving other aspects for exploration at trial, scheduled for January 2009). The court ruled that MDY's "bot" does not violate the DMCA despite the fact WoW has software known as "Warden" designed to scan and deny access to game

servers if such bots are detected on a user's computer. The court reasoned that a user has full access to WoW game client software when the user buys it, and therefore the Glider software does not circumvent any access control.[65]

Although the court rejected Blizzard's DMCA claim, it upheld the copyright and contract claims against MDY.[66] Other aspect of Blizzard's DMCA claim will be tested at trial in January 2009.

Car Product Design Company Attempts to Suppres Competition with EULA

In March 2008, car product design company XPEL Technologies filed suit against American Filter Film Distributors, a rival who provides services for car paint and window film protection. Among a slew of other claims, XPEL alleged that American Filter violated the DMCA by using "Capture" software to copy product images from the XPEL website and distribute the image and product to other auto dealers. XPEL argued the DMCA was violated because (1) the XPEL website is protected by an end-user license agreement (EULA), (2) American Filter clicked that they agreed to the EULA, and (3) the EULA is a technological measure which effectively controls access to the copyrighted design works on XPEL's website. This is the first case where a "click-thru" EULA has been put forward as an access control protected by the DMCA.

In August 2008, the most recent proceedings for this case, American Filter's motion to dismiss the DMCA claim was denied. It will be worth watching this case to see whether XPEL's attempts to transform its EULA into an "access control" will succeed.[67]

6. DMCA Shoulders Aside Computer Intrusion Statutes.

The DMCA's anti-circumvention provisions have also threatened to displace "computer intrusion" and "anti-hacking" laws, something that Congress plainly never intended.

State and federal statutes already protect computer network owners from unauthorized intrusions. These include the Computer Fraud and Abuse Act (CFAA), the Wiretap Act, the Electronic Communications Privacy Act (ECPA), and a variety of state computer intrusion statutes. These statutes, however, generally require that a plaintiff prove that the intrusion caused some harm. The DMCA, in contrast, contains no financial damage threshold, tempting some to use it in place of the statutes that were designed to address computer intrusion.

Fortunately, the courts appear to be taking steps to reign in this particular misuse of the DMCA, ruling that the use of authentic usernames and passwords to access computers cannot constitute circumvention, even if done without the authorization of the computer owner.[68] Until more judicial precedents are on the books, however, the improper use of the DMCA as an all-purpose computer intrusion prohibition will continue to muddy the waters for lawyers and professionals.

Disgruntled Company Sues Former Contractor For Unauthorized Network Access

In April 2003, an automated stock trading company sued a former contract programmer under the DMCA, claiming that his access to the company's computer system over a password-protected virtual private network (VPN) connection was an act of circumvention.

Pearl Investments had employed the programmer to create a software module for its software system. In order to complete the work remotely, the programmer used a VPN to connect to the company's computers. Although the contractor created a very successful software module for the company, the relationship turned frosty after the company ran into financial difficulties and terminated the contractor's contract.

The company sued the contractor when it discovered the contractor's VPN connection to the its system, claiming electronic trespass, as well as violations of computer intrusion statutes, the CFAA, and the DMCA's anti-circumvention provisions. Pearl claimed that it had taken away the authorization it had previously given to the contractor to access its system through the password-protected VPN and that the VPN connection was therefore unauthorized. The Court rejected the company's electronic trespass and CFAA claims due to lack of evidence of any actual damage done. Even though the second server was not being used by the programmer at the time, and its hard drive had been accidentally wiped, the court agreed with Pearl that the *existence* of the VPN was a prohibited circumvention of a technological protection measure that controlled access to a system which contained copyrighted software.[69]

Ticketmaster Sues RMG for Bypassing CAPTCHA

In April 2007, Ticketmaster sued RMG Technologies under the DMCA for circumventing the Ticketmaster website CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart"), the image with distorted letters and numbers that a customer must type before purchasing

a ticket. The website run by RMG Technologies provided tickets to events that were likely to sell out quickly on Ticketmaster. RMG allegedly used software to quickly make bulk purchases of tickets from Ticketmaster, circumventing the limit of four tickets per customer, in order to re-sell the tickets for profit.

Ticketmaster brought suit under the DMCA, the CFAA, the Copyright Act, breach of contract, and under California's criminal code governing computer crimes. On a motion for preliminary injunction, the court found that Ticketmaster was likely to succeed on its DMCA, Copyright Act, and breach of contract claims; however, Ticketmaster would not have been able to prevail on the CFAA claim. (The court found it did not need to address the claim under California's criminal code.)

This ruling illustrates how the DMCA has shouldered aside computer intrusion statutes like the CFAA. Because the CFAA requires that Ticketmaster prove it suffered $5,000 in damages during one year, whereas the DMCA contains no financial damage threshold, Ticketmaster was able to succeed under the DMCA while failing under the CFAA.[70]

The DMCA was not intended for this purpose. The DMCA was designed to protect copyrighted works, not ticket vendors. Although the defense made both these arguments,[71] the court nevertheless ruled in favor of Ticketmaster on the DMCA claim.[72]

Cable Provider Blocks Cable Digital Filters

In addition to computer intrusion statues, the DMCA may also be starting to shoulder aside penal statues in other industry areas.

In August 2008, cable provider CoxCom Inc. successfully forced Jon and Amy Chaffee, and their one employee, to stop selling cable digital filters at computer trade shows. These low-frequency digital filters blocked pay per view charges from being sent to cable companies, thus giving users free pay per view. Not surprisingly, the court granted summary judgment against the Chaffees for violation of the Cable Communications Policy Act, a statute specifically enacted to address theft of cable services to protect the economic viability of cable operators and cable programmers. However, the court also ruled that the Chaffees violated the DMCA.

The DMCA argument is that the Chaffees' low-frequency filters circumvent CoxCom's pay-per-view *billing mechanism*, allegedly a "technological measure" that controls access to copyrighted works. If a billing mechanism has become a "technological measure" within the meaning of the DMCA—it is troubling to think what else may qualify.[73]

7. Conclusion

Years of experience with the "anti-circumvention" provisions of the DMCA demonstrate that the statute reaches too far, chilling a wide variety of legitimate activities in ways Congress did not intend. As an increasing number of copyright works are wrapped in technological protection measures, it is likely that the DMCA's anti-circumvention provisions will be applied in further unforeseen contexts, hindering the legitimate activities of innovators, researchers, the press, and the public at large.

[1] For examples of Congress' stated purpose in enacting the DMCA's anti-circumvention provisions, *see* 144 Cong. Rec. H7093, H7094-5 (Aug. 4, 1998); Senate Judiciary Comm., S. Rep. 105-190 (1998) at 29; Judiciary Comm., H. Rep. 105-551 Pt 1 (1998) at 18; House Commerce Comm., H. Rep. 105-551 Pt 2 (1998) at 38.

[2] *See WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 before the House Subcomm. on Courts and Intellectual Prop.*, 105th Cong., 1st sess. (Sept. 16, 1997) at 62 (testimony of Asst. Sec. of Commerce and Commissioner of Patents and Trademarks Bruce A. Lehman admitting that section 1201 went beyond the requirements of the WIPO Copyright Treaty).

[3] For a full description of the events leading up to the enactment of the DMCA, *see* Jessica Litman, DIGITAL COPYRIGHT 89-150 (2000).

[4] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECHNOLOGY L.J. 519, 537-57 (1999) (http://www.sims.berkeley.edu/~pam/papers.html)

[5] Comment of Edward Felten and J. Alex Halderman, RM 2005-11 – Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Dec. 1, 2005, pages 6-7 (http://www.freedom-to-tinker.com/doc/2005/dmcacomment.pdf).

[6] Recommendation of the Register of Copyrights in RM 2002-4, Oct. 27, 2003, pages 87-89 (http://www.copyright.gov/1201/docs/registers-recommendation.pdf).

[7] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472, 68,477 (Nov. 27, 2006) (http://www.copyright.gov/fedreg/2006/71fr68472.pdf).

[8] Jonathan Band, "Congress Unknowingly Undermines Cyber-Security," S.J. MERCURY NEWS, Dec. 16, 2002; Hiawatha Bray, "Cyber Chief Speaks on Data Network Security," BOSTON GLOBE, October 17, 2002.

[9] Pamela Samuelson, "Anticircumvention Rules: Threat to Science," 293 SCIENCE 2028, Sept. 14, 2001; Letter from Matthew Oppenheim, SDMI General Counsel, to Prof. Edward Felten, April 9, 2001 (http://cryptome.org/sdmi-attack.htm); Felten v. RIAA: EFF Case Archive (http://www.eff.org/IP/DMCA/Felten_v_RIAA/).

[10] John Borland, "Student faces suit over key to CD locks," CNET NEWS, Oct. 9, 2003 (http://news.com.com/Student+faces+suit+over+key+to+CD+locks/2100-1025_3-5089168.html); Declan McCullagh, "SunnComm won't sue grad student," CNET NEWS, Oct. 10, 2003 (http://news.com.com/2100-1027-5089448.html).

[11] Declan McCullagh, "Security Warning Draws DMCA Threat," CNET NEWS, July 30, 2002 (http://news.com.com/2100-1023-947325.html).

[12] John Borland, "Court Blocks Security Conference Talk," CNET NEWS, April 14, 2003 (http://news.com.com/2100-1028-996836.html).

[13] David Becker, "Testing Microsoft and the DMCA," CNET NEWS, April 15, 2003 (http://news.com.com/2008-1082-996787.html); Seth Schiesel, "Behind a Hacker's Book, a Primer on Copyright Law," N.Y. TIMES, July 10, 2003 (http://www.nytimes.com/2003/07/10/technology/circuits/10book.html).

[14] *Mainstream Loudoun v. Board of Trustees*, 24 F.Supp.2d 552 (E.D. Va. 1998).

[15] Jennifer 8 Lee, "Cracking the Code of Online Censorship", N. Y. TIMES, July 19, 2001 (http://www.nytimes.com/2001/07/19/technology/circuits/19HACK.html); Transcript of Hearing in Copyright Office Rulemaking Proceeding RM 2002-04, April 11, 2003, pages 11, 31 (http://www.copyright.gov/1201/2003/hearings/schedule.html); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472, 68,477 (Nov. 27, 2006) (http://www.copyright.gov/fedreg/2006/71fr68472.pdf) (listing "Other Exemptions Considered, But Not Recommended").

[16] ACLU, "In Legal First, ACLU Sues Over New Copyright Law" (http://www.aclu.org/privacy/speech/15201res20020725.html).

[17] Lawrence Lessig, "Jail Time in the Digital Age," N.Y. TIMES, July 30, 2001, page A7. (http://www.nytimes.com/2001/07/30/opinion/30LESS.html); Lisa Bowman, "Elcomsoft Verdict: Not Guilty," CNET NEWS, Dec. 17, 2002 (http://news.com.com/2100-1023-978176.html).

[18] Niels Ferguson, "Censorship in Action: Why I Don't Publish My HDCP Results," Aug. 15, 2001 (http://www.macfergus.com/niels/dmca/cia.html); Niels Ferguson, Declaration in Felten & Ors v R.I.A.A. case, Aug. 13, 2001 (http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_ferguson_decl.html); Lisa M. Bowman, "Researchers Weigh Publication, Prosecution," CNET NEWS, Aug. 15, 2001 (http://news.cnet.com/news/0-1005-200-6886574.html).

[19] Robert Lemos, "Security Workers: Copyright Law Stifles," CNET News, Sept. 6, 2001 (http://news.com.com/2100-1001-272716.html).

[20] Wade Roush, "Breaking Microsoft's e-Book Code," Technology Review, November 2001, page 24.

[21] Jennifer 8 Lee, "Travel Advisory for Russian Programmers," N.Y. Times, Sept. 10, 2001, page C4 (www.nytimes.com/2001/09/10/technology/10WARN.html).

[22] Alan Cox, declaration in Felten v. RIAA, Aug. 13, 2001 (http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_cox_decl.html).

[23] Will Knight, "Computer Scientists Boycott US over Digital Copyright Law," New Scientist, July 23, 2001 (http://www.newscientist.com/article/dn1063.html).

[24] IEEE press release, "IEEE to Revise New Copyright Form to Address Author Concerns," April 22, 2002 (http://www.ieee.org/newsinfo/dmca.html); Will Knight, "Controversial Copyright Clause Abandoned," New Scientist, April 15, 2002 (http://www.newscientist.com/news/news.jsp?id=ns99992169).

[25] *Universal City Studios v. Reimerdes,* 111 F. Supp. 2d. 294 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios v. Corley,* 273 F.3d 429 (2d Cir. 2001).

[26] Carl S. Kaplan, "Questioning Continues in Copyright Suit," N.Y. Times, May 4, 2001 (http://www.nytimes.com/2001/05/04/technology/04CYBERLAW.html); Simson Garfinkel, "The Net Effect: The DVD Rebellion," Technology Review, July/Aug. 2001, page 25 (http://www.simson.net/clips/2001/2001.TR.07.DVDRebellion.pdf); Xenia P. Kobylarz, "DVD Case Clash—Free Speech Advocates Say Copyright Owners Want to Lock Up Ideas; Encryption Code is Key," S.F. Daily J., May 1, 2001.

[27] Subsequent cases have found that using a password in similar circumstances does not violate the DMCA's circumvention ban. *See I.M.S. Inquiry Mgt. Systems v. Berkshire Info. Systems,* 307 F.Supp.2d 521 (S.D.N.Y. 2004).

[28] Declan McCullagh, "Will This Land Me in Jail?", CNET News, Dec. 23, 2002 (http://news.com.com/2010-1028-978636.html).

[29] Julie Cohen, "Call it the Digital Millennium *Censorship* Act – Unfair Use," The New Republic, May 23, 2000 (http://www.law.georgetown.edu/faculty/jec/unfairuse.html).

[30] Robert Lemos, "GameSpy Warns Security Researcher," ZDNet News, Nov. 13, 2003 (http://news.zdnet.com/2100-1009_22-5107305.html).

[31] Lisa M. Bowman, "TiVo Forum Hushes Hacking Discussion," CNET News, June 11, 2001 (http://news.cnet.com/news/0-1005-200-6249739.html).

[32] Regarding hints on evading iTunes Store copy protection, May 7, 2003 (http://www.macosxhints.com/article.php?story=20030507104823670).

[33] EFF, DMCA Triennial Rulemaking: Failing the Digital Consumer, Dec. 1, 2005 (http://www.eff.org/IP/DMCA/copyrightoffice/DMCA_rulemaking_broken.pdf).

[34] Rep. Rick Boucher, "Time to Rewrite the DMCA," CNET News, Jan. 29, 2002 (http://news.com.com/2010-1078-825335.html); Dan Gillmor, "Entertainment Industry's Copyright Fight Puts Consumers in Cross Hairs," S. J. Merc. News, Feb. 12, 2002; Jon Healey & Jeff Leeds, "Record Labels Grapple with CD Protection", L.A. Times, Nov. 29, 2002, C1; John Borland, "Copy-blocked CD Tops U.S. Charts," CNET News, June 17, 2004 (http://news.com.com/Copy-blocked+CD+tops+U.S.+charts/2100-1027_3-5238208.html).

[35] Tim Anderson, "How Apple is Changing DRM," The Guardian, May 15, 2008, Technology News, page 1 (http://www.guardian.co.uk/technology/2008/may/15/drm.apple).

[36] EFF, The Customer Is Always Wrong: A User's Guide to DRM in Online Music, (http://www.eff.org/pages/customer-always-wrong-users-guide-drm-online-music). For information on online music vendors abandoning DRM, *see* Tim Anderson, "How Apple is Changing DRM," The Guardian, May 15, 2008, Technology News, page 1 (http://www.guardian.co.uk/technology/2008/may/15/drm.apple).

[37] Matthew Mirapaul, "They'll Always Have Paris (and the Web)," N.Y. Times, March 16, 2002, page E2; Lisa Bowman, "Hollywood Targets DVD- Copying Upstart," CNET News, Dec. 20, 2002 (http://news.com.com/2100-1023-978580.html); *Paramount Pictures Corp. v. Tritton Technologies Inc.*, No. CV 03-7316 (S.D.N.Y. filed Sept.17, 2003); *321 Studios v. MGM,* 307 F.Supp.2d 1085 (N.D. Cal. 2004).

[38] Recommendation of the Register of Copyrights in RM 2002-4, Oct. 27, 2003, pages 109-26 (http://www.copyright.gov/1201/docs/registers-recommendation.pdf).

[39] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472, 68,474 (Nov. 27, 2006) (http://www.copyright.gov/fedreg/2006/71fr68472.pdf).

[40] EFF, Frequently Asked Questions re *U.S. v. Sklyarov* (http://www.eff.org/IP/DMCA/US_v_Sklyarov/us_v_sklyarov_faq.html).

[41] *RealNetworks, Inc.* v. *Streambox, Inc.,* No. C99-2070P, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

[42] Cease and desist letter from Kenneth Plevan on behalf of Live365.com to John Clegg, developer of Streamripper, April 26, 2001 (http://streamripper.sourceforge.net/dc.php).

[43] Tom Murphy, "embed: DMCA Threats" (http://www.andrew.cmu.edu/~twm/embed/dmca.html); cease and desist letter from Agfa to Murphy (http://www.chillingeffects.org/copyright/notice.cgi?NoticeID=264).

[44] *See Agfa Monotype Corp. v. Adobe Sys.*, 404 F. Supp. 2d 1030 (N.D. Ill. 2005).

[45] Eric Bangeman, "MPAA Sues Over DVD-to-iPod Service," *Ars Technica*, Nov. 17, 2006 (http://arstechnica.com/news.ars/post/20061117-8241.html); Fred von Lohmann, "Movie Studios Sue to Stop Loading of DVDs onto iPods," EFF Deep Links blog, Nov. 16 2006 (http://www.eff.org/deeplinks/2006/11/movie-studios-sue-stop-loading-dvds-ipods).

[46] Ajay Kamalakaran, "U.S. Judge Halts Sales of RealNetworks DVD Software," Reuters, Oct. 9, 2008 (http://www.reuters.com/article/technologyNews/idUSTRE4982C920081009); Greg Sandoval, "Judge Keeps RealDVD Restraining Order In Place," CNET News, Oct. 7, 2008 (http://news.cnet.com/8301-1023_3-10060481-93.html); Press Release, RealNetworks, "RealNetworks Introduces RealDVD: The Best Way to Watch DVDs" (Sept. 8, 2008) (http://www.realnetworks.com/company/press/releases/2008/realdvd.html). The court filings for this case are available at EFF, "RealNetworks v. DVD-CCA (RealDVD case)" (http://www.eff.org/cases/universal-city-studios-v-realnetworks).

[47] Others have also recognized the anti-competitive effects of the DMCA. *See* Timothy B. Lee, "Circumventing Competition: The Perverse Consequences of the Digital Millennium Copyright Act," CATO Policy Analysis No. 564 (Mar. 21, 2006) (http://www.cato.org/pub_display.php?pub_id=6025).

[48] Jennifer Granick, "Free the Cell Phone!," WIRED News, Sept. 30, 2005 (http://www.wired.com/news/culture/0,1284,68989,00.html); Reply Comments of the Wireless Alliance, Copyright Office, Docket No. RM-2005-11 (http://www.copyright.gov/1201/2006/reply/14granick_WAreply.pdf).

[49] David Kravets, "Ruling Allows Cell Phone Unlocking, but Telco Sues Anyway," Wired, Aug. 8, 2007 (http://www.wired.com/politics/onlinerights/news/2007/08/tracfone). For cases brought by Tracfone against phone resellers *see, e.g. TracFone Wireless, Inc. v. Dixon*, 475 F. Supp. 2d 1236 (M.D. Fla. 2007) (ruling in favor of TracFone); *TracFone Wireless, Inc. v. GSM Group, Inc.* 555 F.Supp.2d 1331 (S.D. Fla. 2008) (ruling in favor of TracFone by denying defendant motion to dismiss).

[50] Real has since abandoned DRM for its music download service. *See* Brian Heater & Chloe Albanesius, "Update: Rhapsody DRM-Free Music Targets iTunes," PC Magazine, June 30, 2008 (http://www.pcmag.com/article2/0,2817,2324184,00.asp).

[51] Matt Hines, "'Stunned' Apple rails against Real's iPod move," CNET News, July 29, 2004 (http://news.com.com/'Stunned'+Apple+rails+against+Real's+iPod+move/2100-1041_3-5288378.html); "Real Reveals Real Apple Legal Threat," MacWorld UK, Aug. 10, 2005 (http://www.macworld.co.uk/news/index.cfm?RSS&NewsID=12310); RealNetworks 10-Q filing (May 2005) (http://docs.real.com/docs/investors/V08778.pdf).

[52] Kevin Poulsen, "Hackers Sued for Tinkering with Xbox Games," SecurityFocus, Feb. 9, 2005 (http://www.securityfocus.com/news/10466).

[53] Michael R. Tompkins, "Nikon Encrypts RAW File Data," Imaging Resource, Apr. 20, 2005 (http://www.imaging-resource.com/NEWS/1113977781.html); Declan McCullagh, "Nikon's Photo Encryption Reported Broken," CNET News, Apr. 21, 2005 (http://news.com.com/Nikons+photo+encryption+reported+broken/2100-1030_3-5679848.html).

[54] David Pringle & Steve Stecklow, "Electronics With Borders: Some Work Only in the U.S.," Wall St. J., Jan. 17, 2005, at B1; Reuters, "HP Sued Over Printer Cartridge Expiration," MSNBC, Feb. 22, 2005 (http://www.msnbc.msn.com/id/7012754/).

[55] Fred von Lohmann, "DMCA Used to Stymie Competition … Again," EFF Deep Links blog, Nov. 4, 2005 (http://www.eff.org/deeplinks/archives/004123.php); *Storage Technology v. Custom Hardware Engineering*, 421 F.3d 1307 (Fed. Cir. 2005).

[56] Declan McCullagh, "Lexmark Invokes DMCA in Toner Suit," CNET News, Jan. 8, 2003 (http://news.com.com/2100-1023-979791.html); *Lexmark v. Static Control Components*, 387 F.3d 522 (6th Cir. 2004).

[57] Steve Seidenberg, "Suits Test Limits of Digital Copyright Act," Nat'l L. J., Feb. 7, 2003 (http://www.law.com/jsp/article.jsp?id=1044059435217); *Chamberlain Group v. Skylink Technologies*, 381 F.3d 1178 (Fed.Cir.2004).

[58] Pamela Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised," 14 Berkeley Tech. L.J. 519, 556 (1999) (http://www.sims.berkeley.edu/~pam/papers.html); Testimony of Jonathan Hangartner on behalf of Bleem, Library of Congress, Hearing on DMCA, Stanford University, May 19, 2000, pp. 221-28 (http://www.loc.gov/copyright/1201/hearings/1201-519.pdf).

[59] David Labrador, "Teaching Robot Dogs New Tricks," Scientific American, Feb. 12, 2002 (http://www.sciam.com/article.cfm?articleID=0005510C-EABD-1CD6-B4A8809EC588EEDF&sc=I100322).

[60] "Sony PlayStation ruling sets far-reaching precedent," New Scientist, Feb. 22, 2002 (http://www.newscientist.com/news/news.jsp?id=ns99991933); *Sony Computer Entertainment America Inc.* v. *Gamemasters*, 87 F.Supp.2d 976 (N.D. Cal. 1999); *Stevens v Kabushiki Kaisha Sony Computer Entertainment,* [2005] HCA 58 (Oct. 6, 2005) (http://www.austlii.edu.au/au/cases/cth/high_ct/2005/58.html).

[61] *Davidson & Assoc. v. Jung,* 422 F.3d 630 (8th Cir. 2005); Howard Wen, "Battle.net Goes To War," Salon, April 18, 2002 (http://archive.salon.com/tech/feature/2002/04/18/bnetd/); *Davidson & Assoc. v. Internet Gateway* EFF case archive (http://www.eff.org/IP/Emulation/Blizzard_v_bnetd/).

[62] Declan McCullagh "Apple: Burn DVDs—and We'll Burn You," CNET News, Aug. 28, 2002 (http://news.com.com/2100-1023-955805.html).

[63] *See Macrovision v. Sima Prod. Corp.*, No. 2006-1441, 2006 WL 1063284 (S.D.N.Y. Apr. 20, 2006), *reh'g denied,* 2006 WL 1472152 (S.D.N.Y May 26, 2006), *appeal dismissed* 219 Fed. Appx. 997 (Fed. Cir. Mar. 15, 2007); Nate Anderson, "Digitizing Video Signals Might Violate the DMCA," *Ars Technica*, Aug. 16 2006 (http://arstechnica.com/news.ars/post/20060816-7517.html); Fred von Lohmann, "Another DMCA Misuse: Macrovision v. Sima," EFF Deep Links blog, Aug. 15 2006 (http://www.eff.org/deeplinks/2006/08/another-dmca-misuse-macrovision-v-sima).

[64] Dan Goodin, "Blizzard Awarded $6m in *WoW* Bot Case," Register Hardware, Oct. 1, 2008 (http://www.reghardware.co.uk/2008/10/01/world_of_warcraft_bot_ruling/).

[65] *MDY Industries v. Blizzard,* No. CV-06-2555-PHX-DGC, 2008 WL 2757357 (D. Ariz., July 14, 2008).

[66] *See* Corynne McSherry, "You Bought It, But You Don't Own It," EFF Deep Links blog, July 15, 2008 (http://www.eff.org/deeplinks/2008/07/you-bought-it-you-dont-own-it).

[67] *XPEL Technologies Corp. v. American Filter Film Distributors*, No. SA08-CA0175-XR, 2008 WL 3540345 (W.D. Tex. Aug. 11, 2008); Rebecca Tushnet, "Design, Dastar, (registration) dates and the DMCA," Rebecca Tushnet's 43(B)log, Aug. 17 2008 (http://tushnet.blogspot.com/2008/08/design-dastar-registration-dates-and.html).

[68] *See Egilman v. Keller & Heckman LLP,* 401 F.Supp.2d 105 (D.D.C. 2005); *I.M.S. Inquiry Mgt. Systems v. Berkshire Info. Systems,* 307 F.Supp.2d 521 (S.D.N.Y. 2004).

[69] *Pearl Investments LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326 (D.Me., Apr. 23, 2003).

[70] *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1113 (C.D. Cal. 2007) (". . . because [Ticketmaster] has not quantified its harm as required by the statute or even attempted to show what portion of the harm is attributable to [RMG], the Court cannot find that [Ticketmaster] has affirmatively shown that its harm caused by [RMG] exceeds the $ 5,000 minimum. Thus, the CFAA claim does not provide a basis for a preliminary injunction.").

[71] *Id.* at 1112 ("Defendant's only unique arguments as to the DMCA claim are that CAPTCHA is not a system or a program, but is simply an image, and that CAPTCHA is designed to regulate ticket sales, not to regulate access to a copyrighted work.").

[72] *See id.*; Randall Stross, "Hannah Montana Tickets on Sale! Oops, They're Gone," N.Y. Times, Dec. 16, 2007 (http://www.nytimes.com/2007/12/16/business/16digi.html).

[73] *CoxCom, Inc. v. Chaffee*, 536 F.3d 101 (1st Cir. 2008) (affirming *CoxCom, Inc. v. Chaffee*, No. CA05-107S, 2007 WL 1577708 (D.R.I. May 41, 2007)).