Electronic Frontier Foundation

Unintended Consequences:

Five Years under the DMCA

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 pirates from defeating anti-piracy protections added to copyrighted works, and to ban "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 piracy. As a result, the DMCA has developed into a serious threat to several important public policy priorities:

Section 1201 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.

Section 1201 Jeopardizes Fair Use.

By banning all acts of circumvention, and all technologies and tools that can be used for circumvention, section 1201 grants to copyright owners the power to unilaterally eliminate the public's fair use rights. Already, the music industry has begun deploying "copy-protected CDs" that promise to curtail consumers' ability to make legitimate, personal copies of music they have purchased.

Section 1201 Impedes Competition and Innovation.

Rather than focusing on pirates, many copyright owners have wielded the DMCA to hinder their legitimate competitors. For example, Sony has invoked section 1201 to protect its monopoly on Playstation video game consoles, as well as their "regionalization" system limiting users in one country from playing games legitimately purchased in another.

Section 1201 Becomes All-Purpose Ban on Access To Computer Networks

Further, section 1201 has been misused as a new general-purpose prohibition on computer network access which, unlike the several federal "anti-hacking" statutes that already protect computer network owners from unauthorized intrusions, lacks any financial harm threshold. Disgruntled ex-employer Pearl Investment's use of the DMCA against a contract programmer who connected to the company's computer system through a password-protected Virtual Private Network illustrates the potential for unscrupulous persons to misuse the DMCA to achieve what would not be possible under existing computer access regulation regimes.

This document collects a number of 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.

2. DMCA Legislative Background

Congress enacted section 1201 in response to two pressures. 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 first 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, when Disney's *Tarzan* DVD prevents you from fast-forwarding through the commercials that preface the feature presentation, efforts to circumvent this restriction would be unlawful.

Second, 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 prevent technology vendors from taking steps to defeat the "copy-protection" now appearing on many music CDs, for example.

Section 1201 also 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. Free Expression and Scientific Research

Section 1201 is being used by a number of copyright owners to stifle free speech and legitimate scientific research. The lawsuit against *2600* magazine, threats against Princeton Professor Edward Felten's team of researchers, and prosecution of the Russian programmer Dmitry Sklyarov have chilled a variety of legitimate activities.

Bowing to DMCA liability fears, online service providers and bulletin board operators have begun to censor 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 on existing security protocols. Foreign scientists are increasingly uneasy about traveling to the United States out of fear of possible DMCA liability, and certain technical conferences have begun to relocate overseas.

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.[5]

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."

> Jonathan Band, "Congress Unknowingly Undermines Cyber-Security," S.J. MERCURY NEWS, Dec. 16, 2002. http://www.siliconvalley.com/mld/siliconvalley/4750224.htm
>
> Hiawatha Bray, "Cyber Chief Speaks on Data Network Security," *The Boston Globe,* October 17, 2002. http://www.boston.com/globe/search/

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 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.ß

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

> Pamela Samuelson, "Anticircumvention Rules: Threat to Science," 293 SCIENCE 2028, Sept. 14, 2001. http://www.sciencemag.org/cgi/reprint/293/5537/2028
>
> Letter from Matthew Oppenheim, SDMI General Counsel, to Prof. Edward Felten,

April 9, 2001.
http://cryptome.org/sdmi-attack.htm

Hewlett Packard Threatens SNOsoft

Hewlett-Packard resorted to Section 1201 threats when researchers published their discovery of 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 the DMCA threat received widespread press attention, HP ultimately withdrew the threat. Security researchers received the message, however—publish vulnerability research at your own risk.

Declan McCullagh, "Security Warning Draws DMCA Threat," CNET News, July 30, 2002.
http://news.com.com/2100-1023-947325.html

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. Although the lawsuit complaint Blackboard subsequently filed did not mention the DMCA, its invocation in the original cease-and-desist letter preceding the complaint contributed to the chill the students and conference organizers felt in challenging the complaint and proceeding with the scheduled presentation.

John Borland, "Court Blocks Security Conference Talk," CNET News, April 14, 2003.
http://news.com.com/2100-1028-996836.html

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 commissioned Huang to write the book which analyzes security flaws Huang discovered in the process of reverse-engineering the Microsoft X-Box game console, after Huang published his research as part of his doctoral work at M.I.T. Huang did not distribute the Xbox public security keys which he had isolated through reverse engineering and did not copy any Xbox code. Although the DMCA includes exceptions for circumvention for computer security testing and reverse engineering, they were too narrow to be of use to Huang or his publisher.

Following Microsoft's legal action against the website vendor of an Xbox mod chip in early 2003, and the music industry's 2001 DMCA threats against Professor Felten's research team, Wiley dropped the book fearing that the publisher might be liable for "making available" a "circumvention device." 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. The book is now being published by No Starch Press.

David Becker, *"Testing Microsoft and the DMCA",* CNET News, April 15, 2003.
http://news.com.com/2008-1082-996787.html

Clive Akass, "*Huang Jury on Xbox Cracker*", TechNewsWorld, August 2003
http://www.technewsworld.com/perl/story/31406.html

Seth Schiesel, *"Behind a Hacker's Book, a Primer on Copyright Law",* NEW YORK TIMES, Circuits, July 10, 2003.
http://www.nytimes.com/2003/07/10/technology/circuits/10xbox.html

Censorware Research Obstructed

Seth Finkelstein conducts research on "censorware" software (i.e., programs that block websites that contain objectionable material), working to document flaws in such software, including the products of N2H2, a leading censorware company. Finkelstein's research documenting websites inappropriately blocked by N2H2's software assisted the ACLU's successful First Amendment challenge to the use of mandatory web filtering software by federally-funded public libraries.[6]

N2H2 claims that its encrypted list of blocked websites is legally protected by the DMCA against attempts to read and analyze it. Utilizing a limited three year exemption granted by the Librarian of

Congress and Copyright Register in 2000, Finkelstein circumvented the encryption on the list of sites blocked by BESS in order to analyze flaws in that list.

However, Finkelstein's research work has been severely limited by the fact that the three year exemption is limited to the *act* of circumvention, and does not permit him to create or distribute tools that would facilitate his research. In addition, the existing exemption is due to expire in October 2003, and as Finkelstein testified before the Copyright Office in its 2003 rule-making hearing, unless the exemption is re-granted, Finkelstein will be unable to continue his research because he fears that censorware companies may bring a DMCA lawsuit against him to terminate his research. Even if he were later found not to have violated section 1201, the potential for a DMCA lawsuit would preclude him from undertaking further research.

> Jennifer 8 Lee, "Cracking the Code of Online Censorship", NEW YORK 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, tri-ennial anti-circumvention exemption hearing, April 11, 2003, at pages 11, 31 available at: http://www.copyright.gov/1201/2003/hearings/schedule.html

Benjamin Edelman has also conducted extensive research into flaws in various censorware products. Edelman's research led to his providing expert testimony for the ACLU in a recent federal court case challenging the constitutionality of the Children's Internet Protection Act (CIPA), which mandates that public libraries use censorware products like those sold by N2H2.

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 NH2H 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 3 year exception. As he was not willing to risk civil and criminal penalties under Section 1201, Edelman was forced to go to federal court to seek clarification of his legal rights before he could undertake his legitimate research. However, underscoring the chilling effect of the DMCA on such research, the Court dismissed Edelman's case for lack of standing.

> ACLU, "In Legal First, ACLU Sues Over New Copyright Law" (case archive). http://archive.aclu.org/issues/cyber/Edelman_N2H2_feature.html

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 Co. Ltd. The software allowed owners of Adobe electronic books ("e-books") to convert them from Adobe's e-Book format into Adobe Portable Document Format ("pdf") files, thereby removing restrictions embedded into the files by e-Book publishers.

Sklyarov was never accused of infringing any copyrighted e-Book, nor of assisting anyone else to infringe copyrights. His alleged crime was working on a software tool with many legitimate uses, simply because third parties he has never met might use the tool to copy an e-Book without the publisher's permission.

The Department of Justice ultimately permitted Sklyarov to return home, but elected to proceed against his employer, ElcomSoft, under the criminal provisions of the DMCA. In December 2002, a jury acquitted Elcomsoft of all charges, completing an 18-month ordeal for the wrongly-accused Russian software company.

> Lawrence Lessig, "Jail Time in the Digital Age," N.Y. TIMES at A7, July 30, 2001. 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

Scientists and Programmers Withhold Research

Following the legal threat against Professor Felten's research team and the arrest of Dmitry Sklyarov, a number of prominent computer security experts have curtailed their legitimate research activities out of fear of potential DMCA liability.

For example, prominent Dutch cryptographer and security systems analyst Niels Ferguson discovered a major security flaw in an Intel video encryption system known as High Bandwidth Digital Content Protection (HDCP). He declined to publish his results on his website relating to flaws in HDCP, 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."

> 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

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 content 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.

> Robert Lemos, "Security Workers: Copyright Law Stifles," CNET NEWS, Sept. 6, 2001. http://news.com.com/2100-1001-272716.html

In mid-2001 an anonymous programmer discovered a vulnerability in Microsoft's proprietary e-Book digital rights management code, but refused to publish the results, citing DMCA liability concerns.

> Wade Roush, "Breaking Microsoft's e-Book Code," TECHNOLOGY REVIEW at 24, November 2001. http://www.technologyreview.com/articles/innovation11101.asp

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 U.S. and a number of conference bodies have decided to move their conferences to non-U.S. locations. Russia has issued a travel warning to Russian programmers traveling to the U.S.

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 his concerns about traveling to the U.S. Cox has urged USENIX to hold its annual conference offshore. The International Information Hiding Workshop Conference, the conference at which Professor Felten's team intended to present its original paper, chose to break with tradition and held its next conference outside of the U.S. following the SDMI threat to Professor Felten and his team.

> Will Knight, "Computer Scientists boycott US over digital copyright law," NEW SCIENTIST, July 23, 2001. http://www.newscientist.com/news/news.jsp?id=ns00001063

> Alan Cox of Red Hat UK Ltd, declaration in Felten v. RIAA, Aug. 13, 2001. http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_cox_decl.html

> Jennifer 8 Lee, "Travel Advisory for Russian Programmers," N.Y. TIMES at C4, Sept.10, 2001. http://www.nytimes.com/2001/09/10/technology/10WARN.html

IEEE Wrestles with DMCA

The Institute of Electrical and Electronics Engineers (IEEE), which publishes 30 per cent of all computer science journals worldwide, recently was drawn into the controversy surrounding science and the DMCA. Apparently concerned about possible liability under Section 1201, 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 under the DCMA.

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."

> 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

2600 *Magazine Censored*

The *Universal City Studios* v. *Reimerdes* case[7] illustrates the chilling effect that section 1201 has had on the freedom of the press.

In that case, eight major motion picture companies brought a DMCA suit against *2600* Magazine seeking to block it from publishing the DeCSS software program, which defeats the encryption used on DVD movies. *2600* had made the program available on its web site in the course of 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.

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.

> 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 at 25, July/Aug. 2001. http://www.technologyreview.com/articles/garfinkel0701.asp
>
> Xenia P. Kobylarz, "DVD Case Clash—Free Speech Advocates Say Copyright Owners Want to Lock Up Ideas; Encryption Code is Key," S.F. DAILY JOURNAL, May 1, 2001.

CNET Reporter Feels Chill

Prominent CNET News reporter Declan McCullagh recently found four publicly-available documents on the Transportation Security Administration (TSA) website. The website announced 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." No password was necessary to download the documents, but they were distributed in encrypted form and a password was required to open and read them.

McCullagh obtained the passwords from an anonymous source, but fear of DMCA liability stopped him from reading the documents—using a password without authorization could violate Section 1201. 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."

> Declan McCullagh, "Will This Land Me in Jail?", CNET NEWS, Dec. 23, 2002. http://news.com.com/2010-1028-978636.html

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."

> Julie Cohen, "Call it the Digital Millennium *Censorship* Act – Unfair Use," THE NEW

REPUBLIC, May 23, 2000. http://www.thenewrepublic.com/cyberspace/cohen052300.html

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."

Lisa M. Bowman, "TiVo Forum Hushes Hacking Discussion," CNET NEWS, June 11, 2001. http://news.cnet.com/news/0-1005-200-6249739.html

Mac Forum Censors iTunes 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. This prevents purchasers from playing the songs on non-iPod portable MP3 players or from transferring songs to non Mac OS computers for personal, non-commercial use, even if that would be considered fair use under copyright law. 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.

http://www.macosxhints.com/article.php?story=20030507104823670#comments

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 transformative ways or other 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.

While stopping copyright infringement is an important policy objective, Section 1201 throws out the baby of fair use with the bathwater of digital piracy. By employing technical protection measures to control access to and use of copyrighted works, and using section 1201 litigation against anyone who tampers with those measures, copyright owners can unilaterally eliminate fair use, re-writing the copyright bargain developed by Congress and the courts over more than a century.

Copy-protected CDs

The introduction of "copy-protected" CDs into the marketplace illustrates the collision between fair use and the DMCA. Record labels are aggressively incorporating "copy-protection" on new music releases. Over 10 million copy-protected discs are already in circulation, according to Midbar Technology Ltd, (now Macrovision), one vendor of copy-protection technology. Sony claims that it has released over 11 million copy-protected discs worldwide. Executives from major record labels EMI and BMG have both stated that a significant proportion of all CDs released in the U.S. will be copy-protected by the end of 2003.

Whatever the impact that these copy protection technologies may have on online infringement, they are certain to interfere with the fair use expectations of consumers. For example, copy-protected discs will disappoint the hundreds of thousands of consumers who have purchased MP3 players, despite the fact that making an MP3 copy of a CD for personal use is a fair use. Making "mix CDs" or copies of CDs for the office or car are other examples of fair uses that are potentially impaired by copy-protection technologies.

Companies that distribute tools to "repair" these dysfunctional CDs, restoring to consumers their fair use privileges, run the risk of lawsuits under section 1201's ban on circumvention tools and technologies.

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," SAN JOSE MERCURY NEWS, Feb. 12, 2002. http://www.siliconvalley.com/mld/siliconvalley/2658555.htm

Gwendolyn Mariano, "Copy-Protected CDs Slide Into Stores," CNET NEWS, Feb. 12, 2002.

http://news.com.com/2100-1023-835841.html

Jon Healey and Jeff Leeds, "Record Labels Grapple with CD Protection", LOS ANGELES TIMES, November 29, 2002, C.1. (subscription required for full article) http://www.latimes.com/business/la-fi-secure29nov29.story

Fair Use Tools Banned

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's anti-circumvention provisions, however, prohibit 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 more and more fair uses whittled away by digital locks allegedly intended to "prevent piracy." Perhaps more importantly, **no future fair uses will be developed**—after all, before the VCR, who could have imagined that fair use "time-shifting" of television would become common-place for the average consumer?

Copyright owners argue that these tools, in the hands of copyright infringers, can result in "Internet piracy." But the traditional answer for piracy under copyright law has been to seek out and prosecute the infringers, not to ban the tools that enable fair use. After all, 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.

DeCSS, DVD Copy Plus and DVD CopyWare

Fair use tools have already been yanked off the market. In the *Universal v. Reimerdes* case, discussed above, the court held that Section 1201 bans DeCSS software. This software decrypts DVD movies, making it possible to copy them to a PC. In another case, 321 Studios LLC has filed a declaratory judgment action in San Francisco after being threatened with DMCA liability by the MPAA for distributing DVD Copy Plus, which enables DVD owners to make copies of DVD content. The major motion picture studios have since counter-sued, alleging that DVD copying tools violate the DMCA.

In a separate case, studios Paramount Pictures and Twentieth Century Fox have used the DMCA to sue Tritton Technologies, the manufacturer of DVD CopyWare, and three website distributors of other software that consumers can use to make a copy of the DVDs they have purchased.

There are many legitimate reasons to copy DVDs. Once the video is on the PC, for example, lots of fair uses become possible—film scholars can digitally analyze the film, travelers can load the movie into their laptops, and parents can fast-forward through the "unskippable" commercials that preface certain films. Without the tools necessary to copy DVDs, however, these fair uses become impossible.

Matthew Mirapaul, "They'll Always Have Paris (and the Web)," N.Y. TIMES at E2, March 16, 2002.

Lisa Bowman, "Hollywood Targets DVD-Copying Upstart," CNET News, Dec. 20, 2002. http://news.com.com/2100-1023-978580.html

Paramount Pictures Corporation et al v. Tritton Technologies Inc. et al, No. CV 03-7316 (S.D.N.Y. filed Sept.17, 2003).

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 Adobe's Portable Document Format ("PDF"). This translation process removes the various restrictions (against copying, printing, text-to-speech processing, etc.) that publishers can impose on e-Books. The program is designed to work only with e-Books that have been lawfully purchased from sales outlets.

The Advanced e-Book Processor allowed those who have legitimately purchased e-Books to make fair uses of their e-Books, which would otherwise not be possible with the current Adobe e-Book format. For instance, the program allows people to engage in the following activities, all of which are fair uses:

- read it on a laptop or computer other than the one on which the e-Book was first downloaded;
- continue to access a work in the future, if the particular technological device for which the e-Book 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.

EFF, Frequently Asked Questions re U.S. v. Sklyarov. http://www.eff.org/IP/DMCA/US_v_Sklyarov/us_v_sklyarov_faq.html

Time-shifting and Streaming Media

As more consumers receive audio and video content from "streaming" Internet media sources, they will demand 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 competitor RealNetworks discovered that Streambox had developed a competing streaming media player, it invoked the DMCA and obtained an injunction against the Streambox VCR product.

RealNetworks, Inc. v. *Streambox, Inc.,* 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

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.

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

embed 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.

Tom Murphy, "embed: DMCA Threats." http://www.andrew.cmu.edu/~twm/embed/dmca.html

Cease and Desist letter sent by Agfa. http://www.chillingeffects.org/copyright/notice.cgi?NoticeID=264

5. A threat to innovation and competition

The DMCA is being used to hinder the efforts of legitimate competitors to create interoperable products.

For example, Vivendi-Universal's Blizzard video game division invoked the DMCA in an effort to intimidate the developers of a software product derived from legitimate reverse engineering. Sony has used the DMCA to threaten hobbyists who created competing software for Sony's Aibo robot dog, as well as to sue makers of software that permits the playing of Playstation games on PCs. In each of these cases, the DMCA was used to deter a marketplace competitor, rather than to battle piracy.

Lexmark Sues Over Toner Cartridges

Lexmark, the second-largest printer vendor in the U.S., has long tried to eliminate aftermarket laser printer toner vendors that offer toner cartridges to consumers at prices below Lexmark's. In January 2003, Lexmark employed the DMCA as a new weapon in its arsenal. Lexmark obtained a DMCA injunction banning printer microchip manufacturer Static Control Components from selling chips it claimed were "technology" which "circumvented" certain "authentication routines" between Lexmark toner cartridges and printers.

Lexmark added these authentication routines explicitly to hinder aftermarket toner vendors. Static Control reverse-engineered these measures and sold "Smartek" chips that enabled aftermarket cartridges to work in Lexmark printers. Lexmark used the DMCA to obtain an injunction banning Static Control from selling its reverse-engineered chips to cartridge remanufacturers.[8] Static Control has appealed that decision and countered by filing an anti-trust lawsuit. Whatever the merits of Lexmark's position, it is fair

to say that eliminating the laser printer toner aftermarket was not what Congress had in mind when enacting the DMCA.

> Declan McCullagh, "Lexmark Invokes DMCA in Toner Suit," CNET NEWS, Jan. 8, 2003. http://news.com.com/2100-1023-979791.html

> Steve Seidenberg, "Copyright Owners Sue Competitors," NATIONAL LAW JOURNAL, Feb. 17, 2003. http://www.nlj.com/business/020303bizlede.shtml

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".[9] Chamberlain claimed that Skylink's interoperable clicker violates the DMCA by bypassing an "authentication regime" between the Chamberlain remote opener and the mounted garage door receiver unit.

Skylink reverse engineered the algorithm used by the garage door receiver's computer program. Skylink's transmitter sends three static codes which trigger a resynchronization function and open the garage door. Even though the Skylink clicker does not use the "rolling code" sent by the Chamberlain transmitter, Chamberlain claims that it "bypasses" its "authentication routine" to use the computer program that controls the door's motor. On this view, a consumer who replaced his lost or damaged Chamberlain clicker with one of Skylink's cheaper universal clickers would not he allowed to "access" his own garage. The same argument would apply equally to ban universal remote controls for televisions.

Although Skylink defeated Chamberlain on a motion for summary judgment, Chamberlain has sought to ban the import and sale of Skylink clickers into the U.S. by filing a simultaneous lawsuit against Skylink and the clicker's Chinese manufacturer in the International Trade Commission. Whatever the outcome of that suit, it is clear that in enacting the DMCA, Congress did not intend to give copyright owners the right to veto the creation of interoperable, non-copyrightable goods and technologies.

> Steve Seidenberg, Suits Test Limits of Digital Copyright Act, NATIONAL LAW JOURNAL, February 7, 2003: http://www.law.com/jsp/article.jsp?id=1044059435217

> Katie Dean, "Lexmark: New Fuel for DMCA Foes," WIRED, March 6, 2003: http://www.wired.com/news/digiwood/0,1412,57907-2,00.html

Sony Sues Connectix and Bleem

Since the DMCA's enactment in 1998, Sony has used DMCA litigation to pressure competitors who created software that would allow PC owners to play games intended for the Sony Playstation video game console. In 1999, Sony sued Connectix Corporation, the manufacturer of the Virtual Game Station, an emulator program which allowed Sony Playstation games to be played on Apple Macintosh computers. Sony also sued Bleem, the leading vendor of Playstation emulator software for Windows PCs.

In both cases, Sony claimed, then subsequently withdrew circumvention violations against Sony competitors that had created their products by engaging in legitimate reverse engineering, which has been recognized as noninfringing fair use in a series of Ninth Circuit cases. Connectix, in fact, ultimately won a Ninth Circuit ruling that its reverse engineering was indeed fair use.[10] Both Connectix and Bleem, however, were unable to bear the high costs of litigation against Sony and ultimately were forced to pull their products off the market. Whatever the merits of Sony's position may have been under copyright, trademark, patent, or other legal theories, the competitive efforts of Connectix and Bleem certainly were at a far remove from the "black box" piracy devices that Congress meant to target with section 1201.

> Pamela Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised," 14 BERKELEY TECHNOLOGY L.J. 519, 556 (1999) (discussing the Connectix case). 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

Sony Threatens Aibo Hobbyist

Sony has also invoked the DMCA against a hobbyist who developed custom programs for Sony's Aibo robotic "pet" dog. The hobbyist cracked the encryption surrounding the source code that

manipulates the Aibo to reverse engineer programs that allow owners to customize voice recognition by their Aibos. The hobbyist revealed neither the decrypted source code nor the code he used to defeat the encryption, freely distributed his custom programs, and made no profit. Nevertheless, Sony claimed that the act of circumventing the encryption surrounding the source code 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 will have the rights of commercial development in the programs). The incident, however, illustrated Sony's willingness to invoke the DMCA in situations with no relationship to "piracy."

David Labrador, "Teaching Robot Dogs New Tricks," SCIENTIFIC AMERICAN, Feb. 12, 2002. http://www.sciam.com/explorations/2002/012102aibo/

Blizzard Sues bnetd.org

Section 1201 has been invoked in a federal lawsuit by Vivendi-Universal's Blizzard Entertainment video game division against a group of volunteer game enthusiasts who used reverse engineering to create free and open source software to allow owners of Blizzard games to play the games over the Internet. The software, a server called "bnetd," provides an alternative to Blizzard's own Battle.net servers.

Both Battle.net servers and bnetd servers are available for free and both allow owners of Blizzard games to play with each other across the Internet. The group of volunteers decided to create bnetd to overcome difficulties that they had experienced in attempting to use Battle.net. The bnetd software is freely distributed, open source, and non-commercial.

Blizzard filed suit in St. Louis to bar distribution of bnetd, alleging that the software is a circumvention device that violates the DMCA. According to Blizzard, the bnetd software has been used by some to permit networked play of pirated Blizzard games. Whether or not that is true, the developers are not using the software for that purpose, nor was the software designed for that purpose. The software has numerous legitimate uses for owners of Blizzard games. Whatever else may be said about the bnetd software, it is plainly not a "black box" piracy device. (EFF is representing the bnetd developers.)

Howard Wen, "Battle.net Goes To War," SALON, April 18, 2002. http://archive.salon.com/tech/feature/2002/04/18/bnetd/

EFF case archive. http://www.eff.org/IP/Emulation/Blizzard_v_bnetd/

Sony Attacks Playstation "Mod Chips"

Apart from using the DMCA against vendors of personal computer emulators of Sony's Playstation, Sony has sued a number of manufacturers of so-called "mod chips" for alleged circumvention under the DMCA. In doing so, Sony has been able to enforce a system of geographical regional restrictions that raises significant anticompetitive issues.

So-called "mod chips" are after-market accessories that modify Playstation consoles to permit games legitimately purchased in one part of the world to be played on a games console from another geographical region. Sony has sued mod chip manufacturers in the U.S., the U.K., and Australia. In the U.S., Sony sued Gamemasters, Inc., distributor of the Game Enhancer peripheral device, which allowed U.S. Playstation users 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 banning the use of a technology that would permit users to use legitimately-purchased non-infringing games from other regions.

Recognizing the anti-competitive potential of the region playback control system, the Australian anti-trust authority, the Australian Consumers and Competition Commission intervened in a case Sony ultimately won against an Australian mod chip manufacturer under the Australian equivalent of the DMCA's anti-circumvention provisions.

Sony has argued that mod chips can also be used to enable the use of unauthorized copies of Playstation games. But most Playstation mod chips are not "black box" devices suitable only for piracy. The potential illegitimate uses must be weighed against legitimate uses, such as defeating Sony's region coding system to play games purchased in other countries.

"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).

David Becker, "Sony Loses Australian Copyright Case," CNET News, July 26, 2002. http://news.com.com/2100-1040-946640.html

Apple Harasses Inventive Retailer

When Other World Computing (OWC), a small retailer specializing in Apple Macintosh computers, developed a software patch that allowed all Mac owners to use Apple's iDVD software, they thought they were doing Apple's 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.

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

6. DMCA becomes general purpose ban on computer network access

In a different type of misuse, the DMCA's anti-circumvention provisions have recently been utilized as a general-purpose prohibition on computer network access. Several federal "anti-hacking" statutes already protect computer network owners from unauthorized intrusions. These include the Computer Fraud and Abuse Act, the Wiretap Act, and the Electronic Communications Privacy Act. In addition, the common law doctrine of trespass to chattels has also been widely used for this purpose. However, unlike each of these regimes which seek to balance important public policy goals by only outlawing behavior that meets certain conditions and causes significant financial harm to computer owners, the DMCA contains no financial damage threshold.

Given the very specific existing statutory regimes that regulate this type of behavior, it is clear that Congress did not intend that the DMCA would be used in this way to create a new and absolute prohibition on accessing computer networks in the absence of any type of copyrighted work.

Disgruntled Ex-employer Sues 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 tunnel 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 connected a separate server to the company's server, to which he connected from a VPN tunnel from his office. 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 server connected to the its system, claiming electronic trespass, violation of the anti-hacker legislation, the Computer Fraud and Abuse Act (CFAA) and violation of 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.

As the DMCA has no harm threshold, the anti-circumvention provisions are open to misuse by unscrupulous companies who seek to avoid paying former employees or contractors by revoking authority previously granted and then alleging circumvention.

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

7. Conclusion

Five 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.

EFF would like to thank the following individuals who have helped to create and update this publication: the Samuelson Law, Technology & Public Policy Clinic, Deirdre Mulligan, Nicky Ozer, and Nicolai Nielsen.

---

[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] *See* Professor Ross Anderson, Cambridge University, Declaration in *Felten v. RIAA* (Oct. 22, 2001), describing ways in which the DCMA is suppressing research into security weaknesses in SDMI watermarking technology: (http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011022_anderson_decl.pdf).

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

[7] 111 F. Supp. 2d. 294 (S.D.N.Y. 2000), *aff'd* 273 F.3d 429 (2d Cir. 2001).

[8] *Lexmark International, Inc. v. Static Control Components, Inc*., (E.D. Ky Civil Action No. 02-571 KSF, unreported decision, February 27, 2003), available at EFF's website at: http://www.eff.org/Cases/Lexmark_v_Static_Controls/

[9] *The Chamberlain Group, Inc. v. Skylink Technologies, Inc.,* (N.D. Ill., Civil Action No. 02 C 6376). Complaint, Plaintiff's Motion for Summary Judgment and Defendant's Opposition to Motion for Summary Judgment, available at EFF's website at: http://www.eff.org/Cases/Chamberlain_v_Skylink/

[10] *Sony Computer Entertainment, Inc*. v. *Connectix Corporation,* 203 F.3d 596 (9th Cir. 2000).