Unintended Consequences:

Fifteen Years under the DMCA

March 2013

ELECTRONIC FRONTIER FOUNDATION

Unintended Consequences:

Fifteen 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 is 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

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. The law was ostensibly intended to stop copyright infringers from defeating anti-piracy protections added to copyrighted works.[1]

In practice, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities. As a result, the DMCA has become 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, videogame console accessories, and computer maintenance services. Similarly, Apple has used the DMCA to tie its iPhone and iPod devices to Apple's own software and services.

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. For example, a disgruntled employer used the DMCA against a former contractor for simply connecting to the company's computer system through a virtual private network ("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. Second (as reflected in the details of section 1201, which go well beyond anything the WIPO treaty required),[2] Congress was also responding 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 of a DVD or Blu Ray disc you own for playback on your iPad or smartphone.

The "tools" prohibitions, set out in sections 1201(a)(2) and 1201(b), outlaw the manufacturing, 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 software that was designed to defeat CD copy-protection technologies, 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 criticized as being too narrow to be of use to the constituencies 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 the 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 weaken security for all computer users (including, ironically, for copyright owners counting on technical measures to protect their works), as security researchers shy away from performing and/or sharing research that might run afoul of section 1201.

Activision Shuts Down Videogame Tinkerer

In 2011, publisher Activision released a videogame entitled "Skylanders: Spyro's Adventure." The main selling point of the game was that it shipped with a USB peripheral called the "Portal of Power," which allowed users to scan RFID tags found in real-life toys (also sold by Activision) in order to unlock characters and other objects within the game. Hacker Brandon Wilson was interested in the technology used by the scanner, so he reverse-engineered the device to decrypt its protocols.[5] As soon as he posted his preliminary research online, he received a cease-and-desist letter from Activision.[6]

Activision asserted that Wilson's research might allow users to emulate the "Portal of Power" technology and use it to unlock game content without purchasing the physical Skylanders toys.[7] Brandon responded that he had never published any actual tools for circumventing the "Portal of Power" access controls, nor did he intend to make such tools available.[8] Nonetheless, Activision's threat worked: Brandon removed all his research from his blog and ceased all further work on the project.[9]

Sony Threatens Norwegian website Gitorious

Based in Norway, Gitorious is a platform for open-source programmers to collaborate on new projects.[10] Some projects initiated by Gitorious users involved hacking Sony's PlayStation 3 videogame console for noncommercial, open-source works. As such, some of the projects required the use of the PlayStation 3's root keys. Sony of America sent a letter to Gitorious invoking the DMCA and demanding that Gitorious remove these user's projects from its site.[11] Sony also demanded the identities and private data of the users organizing the projects.[12]

Citing a lack of resources and incentive to fight against Sony, Gitorious complied with the demand, not only removing the targeted projects but also returning an error message for any internal search requests for "playstation," "sony" or "ps3."[13]

The Gitorious story demonstrates how Section 1201 can be used by domestic companies as a club to bully international websites.

Texas Instruments Targets Calculator Hobbyists

In 2009, Texas Instruments (TI) threatened three bloggers with legal action after they posted commentary about a hobbyist's success in reverse engineering the TI-83 Plus graphing calculator.[14] TI's graphing calculators contain technical measures that prevent users from installing alternative operating systems. When a hobbyist reverse engineered this system in order to help others run their own "home brew" operating systems, he wrote about it online. Three bloggers (Brandon Wilson, Tom Cross and Duncan Smith) subsequently posted their own commentary on the results. TI sent the bloggers letters threatening legal action under the DMCA. This despite the fact that there was no hint of "piracy" in the blogger's activities; in fact, TI made the TI-83 Plus software freely available in unencrypted format both online and in the calculators themselves.

Although the bloggers initially complied with TI's demands and removed the content, they subsequently reposted it after EFF responded to TI on their behalf.[15]

Apple Threatens BluWiki

In 2009, Apple threatened the free wiki hosting site BluWiki for hosting a discussion by hobbyists about reverse engineering iPods to interoperate with software other than Apple's own iTunes. Without a work-around, iPod and iPhone owners would be unable to use third-party software, such as Winamp or Songbird, to "sync" their media collections between computer and iPod or iPhone.[16]

The material on the public wiki was merely a discussion of the reverse engineering effort, along with some snippets of relevant code drawn from Apple software. There were no "circumvention tools," nor any indication that the hobbyists had succeeded in their interoperability efforts. Nevertheless, Apple's lawyers sent OdioWorks, the company behind BluWiki, a cease and desist letter threatening legal action under the DMCA.

Bluwiki ultimately sued Apple to defend the free speech interests of its users.[17] In response, Apple dropped its threat, and BluWiki reinstated the deleted pages.[18]

DMCA Delays Disclosure of Sony-BMG "Rootkit" Vulnerability

Professor J. Alex Halderman, then 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.[19] 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 the Librarian of Congress denied their request.[20] In 2006, the Librarian granted an exemption to the DMCA for researchers examining copy protection software on compact discs.[21] However, this exemption, did not protect researchers studying other DRM systems.

In 2009, Prof. Halderman was again forced to seek a DMCA exemption in order to continue his computer security research relating to DRM systems, including the protection mechanisms used on the Electronic Arts videogame, Spore, which has been the subject of class action lawsuits alleging security vulnerabilities.[22] A narrow version of this exemption was granted in 2010.[23] However, the exemption was not renewed in 2012, leaving this research vulnerable to legal action.[24]

SunnComm Threatens Researcher

In October 2003, then 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.[25]

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."[26]

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.[27]

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. A company statement from HP later said its letter to SnoSoft "was not consistent or indicative of HP's policy. We can say emphatically that HP will not use the DMCA to stifle research or impede the flow of information that would benefit our customers and improve their system security." Security researchers got the real message, however—publish vulnerability research at your own risk.[28]

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.[29]

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 then able to get the book published in both print and e-book form by No Starch Press.[30]

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.[31]

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, 2009, or 2012 leaving future researchers without protection from DMCA threats.[32]

Benjamin Edelman has also conducted extensive research into flaws in various censorware products. Edelman's research 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.[33]

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.[34]

Researchers Withhold Work on HDCP

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."[35]

David Wagner, a professor of computer science at the University of California, Berkeley, also found flaws in the HDCP system, but did not publish his findings until several months after the initial discovery.[36] In light of the legal "overhead" associated with his research, Wagner ceased research on copyright protection systems.[37]

Eventually, the HDCP system was cracked, and the master key to the system was posted anonymously to the website pastebin.com, among others.[38] Still, the fear experienced by these researchers was likely justified: in the wake of the crack being posted Intel sent out an angry message threatening *anyone*, including consumers, who used it.[39] This sort of broad threat against consumers is possible because the DMCA's provisions apply to all consumers.

Intel, along with Warner Brothers, followed through on these threats, filing suit against Ohio based Freedom USA, which manufactures devices that decrypt HDCP. Among other legitimate uses, the devices manufactured by Freedom USA allow users with older electronics to connect them to new, HDMI only devices.[40]

Scientists and Programmers Withhold Security Research

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.[41]

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.[42]

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.[43]

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.[44]

The International Information Hiding Workshop Conference, the conference at which Professor Felten's team intended to present its original SDMI watermarking paper, held its 2009 conference outside of the U.S. following the DMCA threat to Professor Felten and his team. It

was not until May 2012 that the conference returned to the United States.[45]

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.[46]

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."[47]

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.[48]

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.[49]

CNET Reporter Feels Chill

CNET News reporter Declan McCullagh confronted the chilling effect of the DMCA firsthand. While researching a story in 2002, 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.

"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."[50]

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 in the comments section of the site. 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." Slashdot refused to comply with Microsoft's demand, and the users' comments remain on the site.[51]

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 an 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. Nonetheless, the research has since been taken down.[52]

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."[53]

Mac Forum Censors iTunes Music Store Discussion

Macintosh enthusiast website Mac OSX Hints 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 at that time were wrapped in Apple's "FairPlay" digital copy protection technology (Apple has since eliminated DRM for digital music downloads and music videos, but has retained it for TV show and movie downloads). 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.[54]

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. Fair use also includes activities undertaken for purposes such as criticism, comment, news reporting, teaching, scholarship or research.

Today, many forms of digital content—including e-books and video—are "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 needed to enable fair uses. As a result, fair uses have been whittled away by digital locks allegedly intended to "prevent piracy." Perhaps more importantly, future fair uses may 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 punishes the innocent as much or more than the guilty.

The DMCA provides for exemptions to the rules, but the process for obtaining those exemptions

is expensive, technical and often fruitless, particularly for consumer fair uses.[55]

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. Although major labels abandoned CD copy-protection after the Sony-BMG "rootkit" scandal in late-2005, more than 15 million copy-protected CDs were distributed.

Such CD copy-protection technologies interfered 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.[56]

Until 2007, authorized digital music download services also utilized DRM systems that frustrated fair use expectations, and technical restrictions remain common for subscription services.[57] And even after music download retailers like iTunes and Amazon.com gave up DRM, consumers who had purchased DRM-restricted files in the past continued to have difficulties as vendors like Walmart shut down the "authentication servers" without which DRM-restricted files could not be transferred to new computers.[58] In other words, rather than prevent piracy, these DRM restrictions have hurt legitimate customers long after they purchased the songs.

Fair Use Tools Banned: DVD/Blu-Ray Copying Tools

There are many legitimate reasons to copy DVDs. Once the video is copied to a computer, for example, lots of fair uses become possible—video creators can remix movie clips into original YouTube videos, frequent travelers can load the movie into their laptops, and DVD owners can skip the otherwise "unskippable" commercials that preface certain films.

DMCA lawsuits targeting makers of DVD copying tools have hampered these and other fair uses. In the *Universal v. Reimerdes* case, discussed above, the court held that the DMCA bans DeCSS, the first of many widely available free tools for decrypting and copying DVDs. 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.[59]

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 have enabled DVD owners to create backups, organize a movie collection digitally, and watch a DVD at any time without being tied to a physical disc. Nor did RealDVD represent a "piracy" threat: RealDVD preserved the DVD's CSS copy-protection system and added numerous additional security measures. RealNetworks also took a license from the DVD Copy Control Association to perform the necessary DVD decryption. Nevertheless, a federal court ruled in August 2009 that, even if the uses enabled by RealDVD were lawful fair uses, the DMCA forbids the distribution of tools like RealDVD.[60]

In light of these rulings, movie fans, film scholars, movie critics, educators, librarians, filmmakers, video remixers, and public interest groups have been forced to ask the Librarian of Congress repeatedly for DMCA exemptions to allow the decryption of DVDs in order to enable noninfringing uses. For example, exemptions have been 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.[61] In 2006, a narrow DMCA exemption was granted to allow film professors to create compilations of motion pictures for educational use in the classroom.[62]

In 2009, educators renewed their request for an exemption that would allow film professors, media studies educators, and students to use short clips taken from DVDs for educational purposes.[63] EFF and the Organization for Transformative Works also applied for an exemption to allow remixers to extract clips from DVDs to create noncommercial remix videos.[64] While the motion picture industry endorsed a renewal of the narrow exemption for film professors, it opposed any expansion to permit other noninfringing uses of DVDs, going so far as to suggest that noninfringing users should camcord DVD clips from flat screen televisions.[65] In a major victory for remixers, educators, and other innovators, the Librarian of Congress finally approved the EFF's request in 2010, and these exemptions were renewed and expanded in 2012.[66]

Even if other 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, even if fair users succeed in obtaining a DMCA exemption, technology companies will remain reluctant to supply them with the necessary circumvention tools.

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.[67]

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.

As described above, Sklyarov was arrested for his work. His alleged crime was his work 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.[[68]]

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 thrive.

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 (years later, this ruling would come to haunt RealNetworks when it found itself the target of a DMCA lawsuit over its own RealDVD software, as described above).[69]

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.[70] As of January 2013, Streamripper remains available for download.[71]

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."

According to Agfa, the fact that embed can be used to allow distribution of protected fonts made it contraband under section 1201, notwithstanding the fact that the tool had many legitimate uses in the hands of hobbyist font developers.[72] As of January 2013, the "embed" program remains available for download on the creator's website.[73]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.[74]

Load-'N-Go Space-shifting

In November 2006, movie studios used the DMCA against 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 them onto her iPod, and then return both the iPod and the original DVDs.

The movie studios claimed this service violated 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. However, the Load-'N-Go service has since become defunct, and the company's website no longer exists.[75]

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, videogame console accessories, and computer maintenance services. Until EFF obtained an exemption for jailbreaking, Apple relied on the DMCA to lock iPhone owners into purchasing software exclusively from Apple's own App Store. 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.[76]

Programmer George Hotz Sued By Sony

Prolific hacker George Hotz, a.k.a Geohot, is well-known for being the first to successfully jailbreak Apple's iPhone. Today, he is perhaps just as famous for his work with Sony's PlayStation 3 and the subsequent legal battle that ensued. In early 2010, Hotz announced that he had gained hypervisor access to the PlayStation 3, allowing him to read and write to the machine's system memory.[77] In creating his hack, Hotz had used encryption research from the failOverflow team, which had previously revealed a security exploit in the system.[78] Hotz's

intention in creating this hack was simply to satisfy his own "curiosity" and to play his own homemade games on the PlayStation 3's hardware.[79] However, Hotz's hack also allowed users to play pirated games on the system. Sony did not take the news well.

Sony's initial response to Hotz's hack was to release a firmware update for all PlayStation 3 consoles. The update, which was mandatory for all users that wished to continue using PlayStation's online services, removed the PlayStation 3's "OtherOS" feature that Hotz had exploited for his hack. (Incidentally, Sony's decision to remove the OtherOS feature led to a separate class action lawsuit initialed against Sony, which has since been dismissed.[80]) In response, Hotz released his *own* custom firmware, and published the root keys that would allow one to crack even the newest PlayStation 3 consoles. At that point, Sony filed suit against Hotz under both the DMCA and CFAA. The researchers at failOverflow were also targeted.

Sony's legal strategy in the Hotz case has been described as "scorched-earth."[81] Not only did Sony seek to impound all "tools of circumvention" (which Sony defined to include even Hotz's research papers), but it also subpoenaed Hotz's PayPal, YouTube, Twitter, and other accounts.[82] Sony also demanded to know the identities of all Internet users who had accessed Geohot's website or YouTube videos while the jailbreak was posted. EFF filed a letter as amicus opposing this extremely broad subpoena.[83]

Eventually, Sony dropped its case against Hotz and the failOverflow team, after Hotz promised not to hack any Sony products, discuss hacking Sony products, or link to any research related to hacking Sony products.[84] Although Hotz has essentially been silenced, his research (and the PlayStation 3 root keys) remain readily accessible on the Internet.

Craigslist Sues Competitors and Innovators

Using the DMCA, Craigslist has sued several cservices that attempted to offer better ways to post ads on Craigslist. In several cases, these suits have forced the competitor to shut down, depriving consumers of a potentially useful service.

In 2009, for example, Craigslist sued Ivan Gasov and Naturemarket, Inc., operators of the website www.powerpostings.com. Gasov and Naturemarket had developed software that permitted users to automatically post ads on Craigslist, and they also offered, for a fee, to post ads to Craigslist on behalf of users. Craigslist had CAPTCHAs ("Completely Automated Public Turing test to tell Computers and Humans Apart"), the images with distorted letters and numbers that a user must type before placing an ad, on their site, and they argued that Gasov and Naturemarket's product circumvented the CAPTCHAs in order to post ads automatically, thus violating the DMCA. The court enjoined Gasov and Naturemarket from using or selling their software and services.[85]

Craigslist has filed numerous similar lawsuits against other services that offer automatic or easier ways to post ads, resulting in the shuttering of these services.[86] Although Craigslist is certainly entitled to use a CAPTCHA to prevent automated access to its site, the DMCA was never intended to give website owners a blunt legal hammer to go after competitors who simply offer new ways to interact with its platform.

Apple Uses DMCA to Lock iPhone to App Store

Apple uses technical measures backed by the DMCA to try to lock iPhone owners into obtaining software ("apps") exclusively from Apple's own iTunes App Store, where every app must be approved by Apple and Apple retains 30% of revenues generated by app sales. Apple also uses the DMCA to prevent iPhone owners from switching to mobile phone carriers of their choice.

Despite Apple's efforts, millions of iPhone owners, assisted by independent hobbyists, have "unlocked" or "jailbroken" their iPhones to use the carriers and apps of their choice. Apple, however, continues to argue that these activities violate the DMCA.[87] The negative consequences for competition and speech have been clear; witness, for example, Apple's rejection of Google's official Google Voice application,[88] and the rejection of apps from Nine Inch Nails[89] and South Park[90] based on "naughty language."

IN 2006 the Librarian of Congress granted an exemption that allowed all users to jailbreak their phones for the purposes of switching carriers. In 2009, The Copyright Office broadened the exemption to legalize all jailbreaking for handsets. In 2012, the EFF sought to preserve the previous exemptions, and to extend the exemption to tablets and videogame consoles.[91] The Librarian decided to preserve the exception for smartphone, but declined to extend the exception further.[92]

Microsoft intimidates Kinect innovators, then backpedals

In 2010, Microsoft launched a new peripheral for its Xbox 360 videogame console. Dubbed the "Kinect," the camera-like USB device was capable of advanced voice and facial recognition, and could capture movement and sound in three dimensions. Given the Kinect's comparatively low price, innovators immediately expressed a desire to use Kinect's technology for projects outside the realm of videogames. However, the device was not initially compatible with any device other than the Xbox 360.

Recognizing the true potential of the technology, Adafruit Industries created a contest, promising to pay a bounty of $1,000 to the first programmer who created an open-source driver for Kinect.[93] Such a driver would give programmers the ability to write their own programs utilizing the Kinect hardware. Microsoft did not approve of Adafruit's contest, writing that "Microsoft does not condone the modification of its products," and that it would "work closely with law enforcement and product safety groups to keep Kinect tamper-resistant."[94]

Despite this veiled DMCA threat, a brave programmer successfully wrote the necessary driver and opened the Kinect for experimentation.[95] Since then, the Kinect has been used for a staggering variety of innovative, futuristic and artistic projects, arguably creating an entirely new technology market.[96] Meanwhile, Microsoft has "done a complete 180 when it comes to hack[ing]," as one website put it.[97] Microsoft announced that it would not pursue legal action against any Kinect hackers.[98] Furthermore, Microsoft claimed that the Kinect was actually *designed* to be open all along; Microsoft planned to release its *own* version of Kinect to be used with Windows.

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 have responded by filing suit under the DMCA. Instead of being used against copyright infringers, the DMCA is being used to prop up the anticompetitive business models of cellular carriers.[99]

At the 2006, and 2009, triennial DMCA rulemaking, the Librarian of congress granted an exemption for cell phone unlocking. Despite this exemption, however, DMCA lawsuits persisted. 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.[100] In 2012, the exemption was not renewed; as of January 26, 2013, cell phone unlocking is once against a DMCA violation.

Apple Ties OS X to Hardware, Targets Psystar

Apple uses technical measures to prevent consumers from installing Apple's OS X operating system onto computers other than those sold by Apple. When Psystar began selling cheaper PCs along with legitimately purchased copies of OS X, it ended up in court facing a DMCA claim by Apple.[101]

In November 2009, a federal judge ruled in favor of Apple on the copyright issues, stating that Psystar's computer infringed Apple's copyright and violated the DMCA. After four years of legal battling and an affirmation from the 9th Circuit, The Supreme Court declined to review Psystar's case.[102] Psystar has now gone out of business, although a number of smaller imitators are springing up to take its place.[103]

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.[104]

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."[105]

As of January 2013, the music and music videos downloaded from iTunes no longer contain DRM, although DRM is still used for downloaded movies and TV shows.[106]

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.[107]

Nikon's Encrypted RAW Format Blocks Adobe

In April 2005, the creator of Adobe's Photoshop software 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, despite the fact that intrepid programmers were able to break the encryption through reverse engineering. Nikon and Adobe ultimately negotiated an agreement, an option that may not be practical for smaller software developers in the future.[108]

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.[109]

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.[110]

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's use of the DMCA was nothing less than an "attempt to leverage its sales into aftermarket monopolies."[111] Now, Chamberlain attempts to limit the use of third party remotes through convoluted "legaleze" printed in its owner's manual.[112]

Microsoft uses DMCA as Counterclaim for Antitrust Lawsuit

Datel, Inc. produces third-party accessories for every major videogame console, including Microsoft's Xbox 360.[113] As with all third-party manufacturers, Datel must engineer its accessories so that they will be compatible with the chosen first-party console; this frequently requires reverse engineering or other hacking. In 2009, Microsoft issued a mandatory firmware update for all Xbox 360 consoles connected to the Internet: this update had no effect on

Microsoft's own memory cards, but rendered Datel's memory cards completely unusable.[114] Datel sued Microsoft for antitrust violations; Microsoft counterclaimed by accusing Datel of violating the DMCA.

It is difficult to imagine a clearer case of the DMCA being used to stifle competition than was the case here. Microsoft forced consumers to purchase its own memory cards and then used the DMCA to attack legitimate competitors. The EFF filed an amicus brief in support of Datel, arguing that the DMCA was not designed to be used to hobble competition and user choice.[115] The case ultimately settled in 2012, but third-party memory cards remain incompatible with the Xbox 360.[116]

Sony Sues Connectix and Bleem

Sony used the 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 and Sega's Dreamcast console.

In both cases, Sony claimed that competitors had violated the DMCA by engaging in unlawful circumvention, even though courts have recognized that the development of interoperable software is 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.[117]

Neither Connectix nor Bleem were able to bear the high costs of litigation against Sony and eventually pulled their products off the market.

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). Nevertheless, Sony discontinued the Aibo robot in 2006.[118] This incident illustrated Sony's willingness to invoke the DMCA in situations with no relationship to "piracy."[119]

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 ramifications 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.[120]

US Government Prosecutes Importers and Distributors of "Mod Chips"

In addition to Sony's attempts to go after manufacturers and distributors of "mod chips," the US government has undertaken criminal prosecutions of "mod chip" importers and distributors. In 2007, as part of "Operation Tangled Web," officers from U.S. Immigration and Customs Enforcement, with assistance from representatives of the software industry, raided 32 locations in 16 states, seeking evidence of the importation of "mod chips" from China.[121]

Although little information about the case has emerged, in 2012 the U.S. Attorney for the Northern District of Ohio indicted 10 people in connection with the case.[122] At least one defendant, William Silvius, charged with violating the DMCA for selling "mod chips," had his indictment upheld by the courts.[123]

Ironically, these indictments went forward as the Copyright Office was considering extending the jailbreaking exception to game consoles, which would legitimize the sale and manufacture of "mod chips," Unfortunately, the Copyright Office declined to extend this exemption beyond phone handsets in its 2012 ruling.

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.[124]

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.[125] Eventually, Apple released iDVD version 6.0 in 2006, which featured full compatibility with external DVD recorders.[126]

Macrovision Sues Sima for Digitizing Analog Video

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 were 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.[127] Although Sima appealed the ruling, it subsequently settled with Macrovision before the appeal was heard.

Blizzard Blocks 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.[128]

The district court ultimately ruled against MDY on Blizzard's DMCA claims, finding that Glider circumvented technical measures used by Blizzard to control access to copyrighted materials stored on the WoW gameservers.[129] The Ninth Circuit agreed, and entered a permanent injunction against MDY to prevent future § 1201(a)(2) violations.[130]

This ruling is troubling because it suggests that software vendors can deploy mechanisms that monitor user behavior and rely on the DMCA to prevent users from "hiding" from these mechanisms. While the prospect of WoW players "cheating" by using Glider may not elicit much sympathy, this precedent could be used to stymie other kinds of innovation among software "add-ons."

Car Product Design Company Attempts to Suppress Competition with the DMCA and a 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 was the first case where a "click-thru" EULA has been put forward as an access control protected by the DMCA.

The court rejected a motion to dismiss the DMCA claim, and the parties subsequently settled the case in October 2008.[131] It remains to be seen whether other plaintiffs follow XPEL's lead in trying to rely on a EULA as an "access control" under the DMCA.

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 in order to bring a civil suit. 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.

Some courts have taken 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.[132] 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 withdrawn 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.[133]

At the subsequent trial, the jury found that the contractor did not violate the DMCA, although the jury did award Pearl Investments $54,000 on other grounds.[134]

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.[135]

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,[136] the court nevertheless ruled in favor of Ticketmaster on the DMCA claim.[137]

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.[138]

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 encrypted software finds its way into an increasing number of devices—from phones to tablets to cars—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), *available at* http://www.sims.berkeley.edu/~pam/papers.html.

[5] Brandon Wilson, *Skylanders portal documentation* (Oct. 27th, 2011 6:35 PM), http://brandonw.net/.

[6] Russell Holly, *Activision Delivers Cease And Desist To Skylanders Tinkerer*, GEEK (Dec. 28, 2011 2:48 PM), http://www.geek.com/articles/games/activision-delivers-cease-and-desist-to-skylanders-tinkerer-20111228/.

[7] Letter from Mark E. Mayer, Mitchel Silberberg & Knupp, LLP, to Brandon L. Wilson (Oct. 26, 2011), *available at* http://brandonw.net/skylanders/activision.pdf.

[8] *See* Letter from Brandon L. Wilson to Mark E. Mayer, Mitchell Silberberg & Knupp LLP, *available at* http://brandonw.net/skylanders/response.txt (last visited June 12, 2012).

[9] *See id.*

[10] *About Gitorious*, GITORIOUS, https://gitorious.org/about (last visited June 12, 2012).

[11] Christian Johansen, *Gitorious receives DMCA takedown notice from Sony*, GITORIOUS (Feb. 2, 2011 1:41 PM), http://blog.gitorious.org/2011/02/02/gitorious-receives-dmca-takedown-notice-from-sony/.

[12] *Id.*

[13] *Id.*

[14] Dan Goodin, *Texas Instruments Aims Lawyers at Calculator Hackers*, THE REGISTER (Sept. 23, 2009), http://www.theregister.co.uk/2009/09/23/texas_instruments_calculator_hacking/.

[15] Letter from EFF to Texas Instruments (Oct. 13, 2009), *available at* http://www.eff.org/files/filenode/coders/TI%20Claim%20Ltr%20101309.pdf; Link to content: http://brandonw.net/calculators/keys/

[16] Robert McMillan, *Apple is Sued after Pressuring Open-Source iTunes Project*, PC WORLD (Apr. 29, 2009), http://www.pcworld.com/article/163909/apple_is_sued_after_pressuring_opensource_itunes_project.html.

[17] Katie Marshal, *Apple Sued for Threatening Wiki Host Over iTunes Code*, APPLE INSIDER (Apr. 27, 2009), http://www.appleinsider.com/articles/09/04/27/apple_sued_for_threatening_wiki_host_over_itunes_code.html.

[18] Thomas Clayburn, *Apple Drops Complaint Against BluWiki*, INFORMATION WEEK (Jul. 22, 2009), http://www.informationweek.com/news/personal_tech/ipod/showArticle.jhtml?articleID=218600244.

[19] 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, 6-7, *available at* http://web.archive.org/web/20061017084037/http://www.freedom-to-tinker.com/doc/2005/dmcacomment.pdf (accessed via the Internet Archive's Wayback Machine).

[20] Recommendation of the Register of Copyrights in RM 2002-4, Oct. 27, 2003, 87-89, *available at* http://www.copyright.gov/1201/docs/registers-recommendation.pdf.

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

[22] Comments of Prof. J. Alex Halderman, *available at* http://www.copyright.gov/1201/2008/comments/halderman-reid.pdf.

[23] *Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works,* U.S. COPYRIGHT OFFICE, http://www.copyright.gov/1201/2010/ (last visited May 30, 2012) (exempting video games from section 1201(a) liability in certain circumstances, such as when circumvention is used solely to find security vulnerabilities in the software).

[24] *See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 77 Fed. Reg. 208 (Oct. 26, 2012) (to be codified at 37 C.F.R. pt. 201), *available at* http://www.copyright.gov/fedreg/2012/77fr65260.pdf.

[25] 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.

[26] Jonathan Band, *Congress Unknowingly Undermines Cyber-Security*, SAN JOSE MERCURY NEWS, Dec. 16, 2002, *available at* http://www.policybandwidth.com/publications/JBand-IPCyberSecurity.pdf; Hiawatha Bray, *Cyber Chief Speaks on Data Network Security*, BOSTON GLOBE, October 17, 2002.

[27] 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, *available at* http://cryptome.org/sdmi-attack.htm; *Felten, et al. v. RIAA, et al.*, EFF, https://www.eff.org/cases/felten-et-al-v-riaa-et-al (last visited Jan. 10, 2013).

[28] Declan McCullagh, *Security Warning Draws DMCA Threat*, CNET NEWS (July 30, 2002), http://news.com.com/2100-1023-947325.html; Kim Zetter, *HP, Bug-Hunters Declare Truce,* PCWORLD (Aug. 9, 2002 3:00 pm), http://www.pcworld.com/article/103853/hp_bughunters_declare_truce.html.

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

[30] David Becker, *Newsmaker: 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; *See Hacking the Xbox,* NO STARCH PRESS, http://nostarch.com/xbox.htm (last visited Jan. 14, 2013).

[31] Mainstream Loudoun v. Bd. of Trs., 24 F.Supp.2d 552 (E.D. Va. 1998), *available at* http://scholar.google.com/scholar_case?case=13796536557265673818.

[32] 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, 11, 31, *available at* 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), *available at* http://www.copyright.gov/fedreg/2006/71fr68472.pdf (listing "Other Exemptions Considered, But Not Recommended"); *Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works*, COPYRIGHT OFFICE, http://www.copyright.gov/1201/2010/ (last visited Jun. 13, 2012).

[33] *In Legal First, ACLU Sues Over New Copyright Law*, ACLU (July 25, 2002), http://www.aclu.org/privacy/speech/15201res20020725.html; *See also* Edelman v. N2H2 Inc., No. 02-CV-11503-RGS (D. Mass. Apr. 7, 2003).

[34] Lawrence Lessig, *Jail Time in the Digital Age*, N.Y. TIMES, July 30, 2001, at A7, *available at* 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.

[35] Niels Ferguson, *Censorship in Action: Why I Don't Publish My HDCP Results*, Aug. 15, 2001, http://web.archive.org/web/20011201184919/http://www.macfergus.com/niels/dmca/cia.html (accessed via the Internet Archive's Wayback Machine); Niels Ferguson, *Declaration in Felten v. R.I.A.A.*, EFF (Aug. 13, 2001), https://w2.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/Researchers-weigh-publication%2C-prosecution/2100-1023_3-271712.html.

[36] *See* Sara Robinson, *Awaiting DMCA Clarification, Researchers Proceed Cautiously*, SIAM NEWS, Volume 35, Number 1, *available at* http://www.siam.org/pdf/news/387.pdf.

[37] *See id.;* E-mail from David Wagner, Professor of Computer Science, University of California, Berkeley, to Declan McCullagh (Nov. 25, 2002 21:56), *available at* http://lists.jammed.com/politech/2002/11/0090.html.

[38] *HDCP Master Key*, http://pastebin.com/SJJELM8S (last visited June 13, 2012).

[39] David Kravets, *Intel Threatens to Sue Anyone Who Uses HDCP Crack*, WIRED (September 17, 2010), http://www.wired.com/threatlevel/2010/09/intel-threatens-consumers/.

[40] *Warner Brothers And Intel Sue Company Over HDCP Circumvention Device*, DIGITAL DIGEST (Dec. 21, 2012, 6:29 PM), http://www.digital-digest.com/news-63556-Warner-Bros-And-Intel-Sue-Company-Over-HDCP-Circumvention-Device.html

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

[42] Wade Roush, *Breaking Microsoft's e-Book Code*, MIT TECHNOLOGY REVIEW (Nov. 1, 2001), http://www.technologyreview.com/web/12645/.

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

[44] Alan Cox, *Declaration in* Felten v. RIAA, EFF (Aug. 13, 2001), https://w2.eff.org/IP/DMCA/Felten_v_RIAA/20010813_cox_decl.html.

[45] Will Knight, *Computer Scientists Boycott US Over Digital Copyright Law,* NEWSCIENTIST (July 23, 2001, 5:42 PM), http://www.newscientist.com/article/dn1063-computer-scientists-boycott-us-over-digital-copyright-law.html; *Previous Information Hiding Venues*, 14TH INFORMATION HIDING CONFERENCE, http://www.ihconference.org/previous_ih.php (last visited May 30, 2012).

[46]*IEEE to Revise New Copyright Form to Address Author Concerns*, THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (April 22, 2002), http://web.archive.org/web/20020424125815/http://www.ieee.org/newsinfo/dmca.html (accessed using the Internet Archive Wayback Machine); Will Knight, *Controversial Copyright Clause Abandoned*, NEWSCIENTIST (April 15, 2002), http://www.newscientist.com/article/dn2169-controversial-copyright-clause-abandoned.html.

[47] *IEEE Drops Reference to DMCA in Revised Authors' Copyright Form*, THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, http://web.archive.org/web/20021103042350/http://www.spectrum.ieee.org/INST/jul02/fdrops.html (accessed using the Internet Archive Wayback Machine).

[48] Universal City Studios v. Reimerdes, 111 F. Supp. 2d. 294 (S.D.N.Y. 2000), *available at* http://scholar.google.com/scholar_case?case=4887310188384829978, aff'd sub nom. Universal City Studios v. Corley, 273 F.3d 429 (2d Cir. 2001), *available at* http://scholar.google.com/scholar_case?case=5930508913825375010.

[49] 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 DVD Rebellion*, MIT TECHNOLOGY REVIEW (July 1, 2001), http://www.technologyreview.com/article/401086/the-dvd-rebellion/; 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.

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

[51] Julie Cohen*, Call it the Digital Millennium Censorship Act – Unfair Use*, THE NEW REPUBLIC ONLINE (May 23, 2000), http://web.archive.org/web/20051213220803/http://www.law.georgetown.edu/faculty/jec/unfairuse.html (accessed via the Internet Archive's Wayback Machine); Link to specifications: Hemos, *Kerberos, PACs And Microsoft's Dirty Tricks*, SLASHDOT (May 2, 2000 03:33PM), http://slashdot.org/story/00/05/02/158204/kerberos-pacs-and-microsofts-dirty-tricks (comments section).

[52] Robert Lemos, *GameSpy Warns Security Researcher*, CNET NEWS (Nov. 13, 2003, 3:29 PM), http://news.cnet.com/2100-7355_3-5107305.html; *See also* CodeWarrior, *Luigi Auriemma finds bugs in Gamespy-DMCA invoked,* DMUSIC (Nov. 12, 2003 9:26PM) http://news.dmusic.com/article/8969.

[53] Lisa M. Bowman, *TiVo Forum Hushes Hacking Discussion*, CNET NEWS (June 11, 2001, 3:15 PM), http://news.cnet.com/TiVo-forum-hushes-hacking-discussion/2100-1023_3-268227.html.

[54] *Regarding Hints on Evading iTunes Store Copy Protection*, MAC OS X HINTS (May 7, 2003 11:29 AM), http://www.macosxhints.com/article.php?story=20030507104823670.

[55] EFF, DMCA TRIENNIAL RULEMAKING: FAILING THE DIGITAL CONSUMER (2005), *available at* http://www.eff.org/IP/DMCA/copyrightoffice/DMCA_rulemaking_broken.pdf.

[56] Rep. Rick Boucher, *Perspective: 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; Jon Healey & Jeff Leeds, *Record Labels Grapple with CD Protection*, L.A. TIMES, Nov. 29, 2002, at C1; John Borland, *Copy-blocked CD Tops U.S. Charts*, CNET NEWS (June 17, 2004), http://news.cnet.com/Copy-blocked-CD-tops-U.S.-charts/2100-1027_3-5238208.html.

[57] *The Customer Is Always Wrong: A User's Guide to DRM in Online Music*, EFF, http://www.eff.org/pages/customer-always-wrong-users-guide-drm-online-music (last visited Jan. 14, 2013). For information on online music vendors abandoning DRM, *see* Tim Anderson, *How Apple is Changing DRM*, THE GUARDIAN (May 15, 2008), http://www.guardian.co.uk/technology/2008/may/15/drm.apple.

[58] Mark Hefflinger, *Walmart to End Support for DRM-Wrapped Songs in October*, DIGITAL MEDIA WIRE (June 1, 2009), http://www.dmwmedia.com/news/2009/06/01/walmart-end-support-drm-wrapped-songs-october.

[59] Matthew Mirapaul, *They'll Always Have Paris (and a Scholarly Web Site)*, N.Y. TIMES (March 16, 2002), http://www.nytimes.com/2002/03/18/movies/arts-online-they-ll-always-have-paris-and-a-scholarly-web-site.html; 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), *available at* http://scholar.google.com/scholar_case?case=8541119834567462882).

[60] Real Networks, Inc. v. DVD Copy Control Ass'n, 641 F. Supp. 2d 913, 942 (N.D. Cal., 2009), *available at* http://www.eff.org/files/filenode/RealDVD/Real%20v%20DVD-CCA%2C%20PI%20Order%20081109.pdf).

[61] COPYRIGHT OFFICE, RECOMMENDATION OF THE REGISTER OF COPYRIGHTS IN RM 2002-4, 109-26 (2003), *available at* http://www.copyright.gov/1201/docs/registers-recommendation.pdf.

[62] *Statement of the Librarian of Congress Relating to Section 1201 Rulemaking*, COPYRIGHT OFFICE (Nov. 27, 2006), http://www.copyright.gov/1201/docs/2006_statement.html.

[63] Comments of Renee Hobbs, Peter Decherney, Library Copyright Alliance, *available at* http://www.copyright.gov/1201/2008/index.html.

[64] Comments of EFF and OTW, *available at* http://www.copyright.gov/1201/2008/comments/lohmann-fred.pdf.

[65] Jacqui Cheng, *MPAA: Teachers Should Videotape Monitors, Not Rip DVDS*, ARS TECHNICA (May 7, 2009), http://arstechnica.com/tech-policy/news/2009/05/mpaa-teachers-should-video-record-tv-screens-not-rip-dvds.ars.

[66] *2009 DMCA Rulemaking*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/cases/2009-dmca-rulemaking (last visited June 7, 2012); *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 77 Fed. Reg. 208 (Oct. 26, 2012) (to be codified at 37 C.F.R. pt. 201), *available at* http://www.copyright.gov/fedreg/2012/77fr65260.pdf.

[67] *US v. ElcomSoft & Sklyarov FAQ*, EFF (Feb. 19, 2002, 2:35 PM), https://www.eff.org/pages/us-v-elcomsoft-sklyarov-faq#AboutEBooks

[68] Lisa Bowman, *Elcomsoft Verdict: Not Guilty*, CNET NEWS (Dec. 17, 2002), http://news.com.com/2100-1023-978176.html.

[69] RealNetworks, Inc. v. Streambox, Inc., No. C99-2070P, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000), *available at* http://legal.web.aol.com/decisions/dlip/realorder.pdf.

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

[71] *Welcome to Streamripper*, STREAMRIPPER, http://streamripper.sourceforge.net/ (last visited Jan. 10, 2013).

[72] Tom Murphy, *embed: DMCA Threats*, TRUETYPE EMBEDDING-ENABLER: DMCA THREATS, http://web.archive.org/web/20020806073714/http://www.andrew.cmu.edu/~twm/embed/dmca.html (accessed via the Internet Archive's Wayback Machine) (last visited Jan. 14, 2013); Cease and desist letter from Agfa to Tom Murphy, *available at* http://www.chillingeffects.org/copyright/notice.cgi?NoticeID=264.

[73] *See Truetype embedding-enabler*, http://carnage-melon.tom7.org/embed/ (last visited Jan. 10, 2013).

[74] *See* Agfa Monotype Corp. v. Adobe Sys., 404 F. Supp. 2d 1030 (N.D. Ill. 2005), *available at* http://scholar.google.com/scholar_case?case=502109184695805642).

[75] 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; *See* Greg Sandoval, *Movie studios sue DVD-to-iPod service*, CNET NEWS (Nov 17, 2006 3:30 PM), http://news.cnet.com/Movie-studios-sue-DVD-to-iPod-service/2100-1030_3-6136806.html.

[76] 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, *available at* http://www.cato.org/pub_display.php?pub_id=6025.

[77] Jonathan Fildes, *PlayStation 3 'hacked' by iPhone cracker*, BBC (Jan. 25, 2010), http://news.bbc.co.uk/2/hi/technology/8478764.stm.

[78] George Hotz, *Geohot Releases dePKG – Firmware Package Decrypter*, PSXSCENE (Dec. 30, 2010), http://web.archive.org/web/20110715131242/http://psx-scene.com/forums/f6/geohot-releases-depkg-firmware-package-decrypter-74094/?s=22e8521743f1afe445584774f1386361 (accessed via the Internet aAchive's Wayback Machine).

[79] Fildes, *supra* note 77.

[80] In re Sony PS3 Other OS Litig., 828 F. Supp. 2d 1125 (N.D. Cal. 2011).

[81] David Kravets, *Sony Settles PlayStation Hacking Lawsuit,* WIRED (Apr. 11, 2011), http://www.wired.com/threatlevel/2011/04/sony-settles-ps3-lawsuit

[82] Corynne McSherry & Marcia Hofmann, *Sony v. Hotz: Sony Sends A Dangerous Message to Researchers -- and Its Customers*, FF (Jan. 19, 2011), https://www.eff.org/deeplinks/2011/01/sony-v-hotz-sony-sends-dangerous-message.

[83] Letter from Corynne McSherry, Electronic Frontier Foundation, to Magistrate Judge Joseph C. Spero, United States District Court, Northern District of California, (Feb. 24, 2011), *available at* http://www.wired.com/images_blogs/threatlevel/2011/03/effletter.pdf.

[84] Corynne McSherry, *Sony v. Hotz Ends With a Whimper, I Mean a Gag Order*, FF(Apr. 12, 2011), https://www.eff.org/deeplinks/2011/04/sony-v-hotz-ends-whimper-i-mean-gag-order.

[85] Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039, 1050 (N.D. Cal. 2010)

[86] *See, e.g.*, Craigslist, Inc., v. Mesiab, No. C 08–05064 CW (N.D. Cal. 2010); Craigslist, Inc., v. Kerbel, No. C–11–3309 EMC (N.D. Cal. 2012); Craigslist, Inc. v. Hubert, 278 F.R.D. 510 (N.D. Cal. 2011); Craigslist, Inc. v. Branley, No. 11–3545 SC (N.D. Cal. 2012).

[87] David Kravets, *Apple v. EFF: The iPhone Jailbreaking Showdown*, WIRED (May 2, 2009), http://www.wired.com/threatlevel/2009/05/apple-v-eff-the-iphone-jailbreaking-showdown/.

[88] Jason Kincaid, *Apple is Growing Rotten to the Core: Official Google Voice App. Blocked from App Store*, TECHCRUNCH (Jul. 27, 2009), http://techcrunch.com/2009/07/27/apple-is-growing-rotten-to-the-core-and-its-likely-atts-fault/.

[89] Chris Matyszczyk, *Apple Rejects Nine Inch Nails iPhone Apps Update*, CNET NEWS (May 2, 2009), http://news.cnet.com/apple-rejects-nine-inch--nails-iphone-app-update/.

[90] Fred von Lohmann, *Another iPhone App Banned: Apple Deems South Park App 'Potentially Offensive*, EFF DEEP LINKS BLOG (Feb. 17, 2009), http://www.eff.org/deeplinks/2009/02/south-park-iphone-app-denied.

[91] *See Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works*, COPYRIGHT OFFICE, http://www.copyright.gov/1201/2010/ (last visited Jun. 13, 2012).

[92] *See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 77 Fed. Reg. 208 (Oct. 26, 2012) (to be codified at 37 C.F.R. pt. 201), *available at* http://www.copyright.gov/fedreg/2012/77fr65260.pdf.

[93] Daniel Terdiman, *Bounty offered for open-source Kinect driver*, CNET NEWS (Nov. 4, 2010 12:50 PM), http://news.cnet.com/8301-13772_3-20021836-52.html.

[94] *Id.*

[95] *WE HAVE A WINNER – Open Kinect driver(s) released – Winner will use $3k for more hacking – PLUS an additional $2k goes to the EFF!,* ADAFRUIT (Nov. 10, 2010 2:51 PM), http://www.adafruit.com/blog/2010/11/10/we-have-a-winner-open-kinect-drivers-released-winner-will-use-3k-for-more-hacking-plus-an-additional-2k-goes-to-the-eff/

[96] Rob Walker, *Freaks, Geeks and Microsoft: How Kinect Spawned a Commercial Ecosystem*, THE NEW YORK TIMES (May 31, 2012), http://www.nytimes.com/2012/06/03/magazine/how-kinect-spawned-a-commercial-ecosystem.html?pagewanted=1&_r=2.

[97] *Id.*

[98] *Kinect for Windows: Overview*, MICROSOFT, http://www.microsoft.com/en-us/kinectforwindows/purchase/overview.aspx (last visited June 12, 2012).

[99] Jennifer Granick, *Free the Cell Phone!*, WIRED (Sept. 30, 2005), http://www.wired.com/politics/law/commentary/circuitcourt/2005/09/68989; Reply Comments of the Wireless Alliance, Copyright Office, Docket No. RM-2005-11, *available at* http://www.copyright.gov/1201/2006/reply/14granick_WAreply.pdf.

[100] 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), *available at* http://scholar.google.com/scholar_case?case=12046901395060506289; 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), *available at* http://scholar.google.com/scholar_case?case=6094189997003869052); TracFone Wireless, Inc. v. SND Cellular, Inc., 715 F. Supp. 2d 1246 (S.D. Fla. 2010) (awarding TracFone statutory damages in the amount of $11,370,000 under the DMCA).

[101] Gregg Keizer, *Apple Adds DMCA Charge to Lawsuit Against Psystar*, COMPUTERWORLD (Nov. 30, 2008), http://www.computerworld.com/s/article/9121798/Apple_adds_DMCA_charge_to_lawsuit_against_Psystar.

[102] Josh Lowensohn, *Supreme Court Denies Psystar's Appeal In Mac Clone Case*, CNET NEWS (May 14, 2012 8:25 PM), http://news.cnet.com/8301-13579_3-57434212-37/supreme-court-denies-psystars-appeal-in-mac-clone-case/.

[103] Gregg Keizer, Judge's Ruling Puts Legal Nail in Psystar's Coffin, COMPUTERWORLD (Nov. 14, 2008), http://www.computerworld.com/s/article/9140878/Judge_s_ruling_puts_legal_nail_in_Psystar_s_coffin?taxonomyId=146&pageNumber=1; David Winograd, *Psystar Is Dead. Long Live Quo Computer*, TUAW (Sep. 10, 2010 9:00AM), http://www.tuaw.com/2010/09/10/psystar-is-dead-long-live-quo-computer/.

[104] 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.

[105] 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), *available at* http://docs.real.com/docs/investors/V08778.pdf.

[106] Macworld Staff, *iTunes Store and DRM-free music: What you need to know*, MACWORLD (Jan. 7, 2009), http://www.macworld.com/article/1138000/drm_faq.html.

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

[108] 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.

[109] Fred von Lohmann, *DMCA Used to Stymie Competition ... Again*, EFF DEEP LINKS BLOG (Nov. 4, 2005), https://www.eff.org/deeplinks/2005/11/dmca-used-stymie-competition-again; Storage Technology v. Custom Hardware Engineering, 421 F.3d 1307 (Fed. Cir. 2005), *available at* http://scholar.google.com/scholar_case?case=5265572440015937430.

[110] 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), *available at* http://scholar.google.com/scholar_case?case=18217592195742478731.

[111] 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), *available at* http://scholar.google.com/scholar_case?case=16927618869037195909).

[112] Mike Masnick, *Losers Of Garage Door DMCA Case Try To Use Legaleze To Lock Up Your Garage Door Openers Anyway,* TECHDIRT (Dec. 18, 2009 6:35 PM), http://www.techdirt.com/articles/20091217/0152127402.shtml

[113] Ben Doernberg, *Microsoft Argues that Third-Party Peripherals are Illegal*, PUBLIC KNOWLEDGE (Jun. 23, 2011) http://www.publicknowledge.org/blog/microsoft-argues-third-party-peripherals-are-.

[114] Mike Masnick, *Microsoft Still Claiming That It Can Use The DMCA To Block Competing Xbox Accessories*, TECHDIRT (Jun. 21, 2011 7:20 AM), http://www.techdirt.com/articles/20110620/10505614766/microsoft-still-claiming-that-it-can-use-dmca-to-block-competing-xbox-accessories.shtml.

[115] *See* Brief Of Amici Curiae Electronic Frontier Foundation And Public Knowledge In Support Of Datel's Motion For Summary Judgment at 3, *Datel Holdings Ltd. v. Microsoft Corp.*, No. 09-cv-5535 (N.D. Cal 2011), *available at* https://www.eff.org/files/filenode/datel_v_microsof/datelamicus61511.pdf.

[116] *Microsoft, Datel Settle Lawsuits,* GAMEPOLITICS (Jan. 4, 2012), http://gamepolitics.com/2012/01/04/microsoft-datel-settle-lawsuits.

[117] 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) , *available at* 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, at 221-28, *available at* http://www.loc.gov/copyright/1201/hearings/1201-519.pdf.

[118] John Borland, *Sony Puts Aibo to Sleep*, CNET NEWS (Jan. 26, 2006 5:11 PM), http://news.cnet.com/2100-1041_3-6031649.html.

[119] David Labrador, *Teaching Robot Dogs New Tricks*, SCIENTIFIC AMERICAN (Feb. 12, 2002), http://www.scientificamerican.com/article.cfm?id=teaching-robot-dogs-new-t&sc=I100322.

[120] Barry Fox, *Sony PlayStation Ruling Sets Far-Reaching Precedent*, NEW SCIENTIST (Feb. 22, 2002, 12:14 PM), http://www.newscientist.com/article/dn1933-sony-playstation-ruling-sets-farreaching-precedent.html; Sony Computer Entertainment America Inc. v. Gamemasters, 87 F.Supp.2d 976 (N.D. Cal. 1999), *available at* http://scholar.google.com/scholar_case?case=8151910487264729114); Stevens v Kabushiki Kaisha Sony Computer Entertainment, [2005] HCA 58 (Oct. 6, 2005), *available at* http://www.austlii.edu.au/au/cases/cth/high_ct/2005/58.html.

[121] *Feds' Mod Chip Raid Ended a $2.5 Million Piracy Operation*, GAMEPOLITICS.COM (Nov. 24, 2008), http://gamepolitics.com/2008/11/24/feds039-mod-chip-raid-ended-25-million-piracy-operation#.UO8KVHeCcvk.

[122] Zachary Knight, *After Four Years Feds Finally Get Aroung to Prosecuting Ten Mod Chip Sellers*, TECHDIRT (May 2, 2012, 10:02 AM), http://www.techdirt.com/articles/20120430/17092418721/after-four-years-feds-finally-get-around-to-prosecuting-ten-mod-chip-sellers.shtml

[123] U.S. v. Silvius, No. 1:12CR172, slip. op. (N. D. Ohio Nov. 21, 2012), *available at* http://scholar.google.com/scholar_case?case=7116564093458068957&hl=en&as_sdt=2,5&as_vis=1)

[124] Davidson & Assoc. v. Jung, 422 F.3d 630 (8th Cir. 2005); Howard Wen, *Battle.net Goes To War*, SALON (April 18, 2002), http://www.salon.com/2002/04/18/bnetd/; *Blizzard v. BNETD*, EFF, https://www.eff.org/cases/blizzard-v-bnetd (last visited Jan. 14, 2013).

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

[126] Tony Smith, *How to Get iDVD to Work with an External Burner*, EHOW TECH, http://www.ehow.com/how_5244118_idvd-work-external-burner.html (last visited June 7, 2012) ("With the release of iDVD 6.0, as part of iLife '06, Apple finally included the often-requested ability to burn DVDs to an external CD drive.").

[127] *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.

[128] Dan Goodin, *Blizzard Awarded $6m in WoW Bot Case*, REGISTER HARDWARE (Oct. 1, 2008), http://www.reghardware.com/2008/10/01/world_of_warcraft_bot_ruling/.

[129] MDY Industries, LLC. V. Blizzard Ent., Inc., 616 F. Supp. 2d 958, 966 (D. Ariz. Jan 28, 2009), *available at* http://scholar.google.com/scholar_case?case=321636840809513184.

[130] MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 954 (9th Cir. 2010), as amended on denial of reh'g (Feb. 17, 2011), opinion amended and superseded on denial of reh'g, 09-15932, 2011 WL 538748 (9th Cir. Feb. 17, 2011).

[131] 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.

[132] *See* Egilman v. Keller & Heckman LLP, 401 F.Supp.2d 105 (D.D.C. 2005), *available at* http://scholar.google.com/scholar_case?case=12998125146086841657; I.M.S. Inquiry Mgt. Systems v. Berkshire Info. Systems, 307 F.Supp.2d 521 (S.D.N.Y. 2004), *available at* http://scholar.google.com/scholar_case?case=12954155286023485320.

[133] Pearl Investments LLC v. Standard I/O, Inc., 257 F. Supp. 2d 326 (D.Me., Apr. 23, 2003), *available at* http://scholar.google.com/scholar_case?case=10485186593853024142).

[134] Pearl Investments, LLC v. Standard I/O, Inc., 324 F. Supp. 2d 43, 45 (D. Me. 2004), *available at* http://scholar.google.com/scholar_case?case=1439987705010697232.

[135] 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."), *available at* http://scholar.google.com/scholar_case?case=14769750588422384913.

[136] *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."), *available at* http://scholar.google.com/scholar_case?case=3981873387095830655.

[137] *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.

[138] 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)).