

**The Digital Millennium Copyright Act:
A Threat to Legitimate Scientific Research,
Copyright Holders, and Democracy Itself.**

Christopher Soghoian

**Johns Hopkins University
Information Security Institute
Rights in the Digital Age
December 16, 2003**

Table of Contents

Introduction.....	4
DMCA Background.....	4
A Powerful Tool Used to Threaten Researchers.....	6
<i>Felten et al v. RIAA</i>	7
Swarthmore Coalition for the Digital Commons vs. Diebold Election Systems.....	8
John Halderman vs. SunnComm Technologies.....	9
The Stifling Effect on Legitimate Scientific Research.....	10
Niels Ferguson vs. the DMCA.....	11
Other Research Kept Quiet.....	12
Foreign Researchers Are Boycotting the U.S.....	12
Conclusion.....	13
References.....	15

Introduction

Congress created the Digital Millennium Copyright Act in 1998 in order to protect the works of artists from acts of piracy and theft that the Internet and other new technologies made easy. Congress did not foresee, and certainly did not intend for it to be used to stifle legitimate scientific research, and to scare foreign researchers from entering the country. Powerful corporations, armed to the teeth with teams of lawyers, are using the DMCA to suppress the details of security flaws in their products. In doing so, they hurt the scientific community, and expose copyright owners to serious risk by suppressing the truth about flaws in products that they rely on to protect their works [Cox].

DMCA Background

On October 28th 1998, President Clinton signed the DMCA into law. The Act is designed to implement the WIPO Copyright Treaty (WCT), signed in December 1996 at the World Intellectual Property Organization (WIPO) Geneva conference [UCLA]. The DMCA is split into five titles, but only title I, the “WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998”, is relevant to the issues discussed in this paper.

Article 11 of the WCT states: “Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their

rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.”

In his testimony before the House Subcommittee on Courts and Intellectual Property, Bruce A. Lehman, Assistant Secretary of Commerce and Commissioner of Patents and Trademarks, admitted that section 1201 went far beyond the requirements of the WIPO Copyright Treaty [EFF1].

During the DMCA debate in the House of Representatives, Representative Barney Frank stated that the purpose of the law was to counter “technological change[s] which makes it easier for that minority of people who do not respect others' intellectual property to steal it because of the [...] Internet. [We wanted] to come up with ways to adapt the protection of intellectual property to a modern technological era without unduly diminishing people's rights to enjoy things” [Frank]. Congressional supporters also indicated that the legislation was carefully drafted to only go after so-called “black boxes” (devices whose sole purpose was infringement) and that multi-use technologies could continue to be made and sold [BTLJ]. It is clear that Congress went beyond its treaty obligations to meet the concerns of copyright owners who were worried about new digital threats to their copyrighted works.

Title I, §103 of the DMCA adds §1201 to the Copyright Act. This new section implements the obligation to provide “adequate and effective protection against circumvention of technological measures used by copyright owners to protect their works” [LOC]. §1201(a)(1) outlaws the act of circumventing technological measures put in place by copyright holders to control access to their works. §1201(a)(2) and §1201(b) prohibit the manufacture, sale, distribution or trafficking of tools and technologies that

make those acts possible. For example, while it would be a violation of the former section for an individual to bypass encryption scheme used to copy protect DVDs, it would violate the latter two sections if that individual shared the technique or a tool implementing that technique with anyone else.

Due to concerns raised by those in industry and academia, Congress included a series of exemptions to §1201, which allow circumvention for: nonprofit library use, archive and educational institution use, reverse engineering of software for the purpose of achieving interoperability with other programs, encryption research, protection of minors, personal privacy and security testing. The Librarian of Congress is also given the power to set additional exceptions to respond to changing technology and public attitudes.

While those exemptions were intended to protect legitimate research, as the co-chairs of the Association of Computing Machinery explained in a letter to the Senate Subcommittee on Technology, Terrorism, and Government Information, “exempting encryption research from the anti-circumvention provisions is too limited as the majority of computer security research does not involve encryption” and that, “permitting reverse engineering for the sole purpose of interoperability may criminalize development of software engineering tools and technology with other uses” [ACM].

A Powerful Tool Used to Threaten Researchers

The DMCA has given copyright owners a powerful tool that many are using to gag scientific research, and to silence the free speech of researchers and activists. As the following examples will show, the scientific community, the American democratic

system, and the security and thus the wellbeing of the Internet are at grave risk due to DMCA abuses.

Felten et al v. RIAA

In September 2000, the Secure Digital Music Initiative (SDMI), a consortium of music-industry companies, announced a “public challenge” in an “Open Letter to the Digital Community” [Felten 1] in which it invited members of the public to try to break certain data-encoding copy protection technologies that SDMI members had developed. Princeton professor Dr. Edward Felten, and researchers from Rice and Xerox took up the challenge, broke the scheme and instead of submitting their results to SDMI in exchange for a small cash prize, chose to forgo the prize and publish their research [Cryptome].

As the researchers prepared to submit their research to an academic conference they, their employers and the conference organizers received DMCA cease and desist letters from the SDMI legal team, stating that even though “the purpose of releasing your research is not designed to help anyone impose or steal anything” and that while “[your] participation in the challenge and your contemplated disclosure appears to be motivated by a desire to engage in scientific research that will ensure that SDMI does not deploy a flawed system”, it “could result in significantly broader consequences and could directly lead to the illegal distribution of copyrighted material [...] and would [therefore] subject your research team to enforcement actions under the DMCA and possibly other federal laws.”

It was only after the Electronic Frontier Foundation (EFF) filed suit on behalf of Dr. Felten the recording industry backed down and assured the researchers that they were safe from legal harassment [Felten 2]. Based on this experience, the Information Hiding Workshop committee, to which the researchers first attempted to submit their research, decided to stop holding their annual conference in the United States [Anderson].

Swarthmore Coalition for the Digital Commons vs. Diebold Election Systems

In March 2003, an anonymous hacker broke into the computer network of Diebold Election Systems, a leading manufacturer of electronic voting machines, and stole 15,000 internal company memos revealing that the company had been aware of security flaws in its e-voting software for years, but sold the faulty systems to state governments anyway [Wired 1]. In August, electronic-voting activists posted the memos to their personal websites. Shortly after, some of the electronic media took notice.

In July 2003, Johns Hopkins and Rice University researchers released a scathing report on the source code for Diebold's machines that had accidentally been placed on one of the company's publicly accessible servers. The researchers found a number of serious flaws in the software, stating in their report that "this voting system is far below even the most minimal security standards applicable in other contexts." They also noted "as a society, we must carefully consider the risks inherent in electronic voting, as it places our very democracy at risk" [Rubin]. As a result of the report, Diebold began receiving significant press coverage, and several governors publicly contemplated suspending orders for additional voting machines [Wired 2].

Beginning in August, Diebold began sending DMCA cease and desist letters to more than a dozen individuals who either posted the memos, or links to other sites that hosted them [Wired 3]. Diebold's lawyers stated that the documents revealed proprietary information about the workings of its e-voting system that would benefit its competitors, yet at the same time asserted that the fact that the company sent the cease-and-desist letters did not mean the documents were authentic [Mercury]. By asserting that the stolen material was their copyrighted property, yet at the same time claiming that the material might not be theirs, it appears they were trying to use the legal system to proverbially have their cake and eat it too.

While many of the original memo posters caved in to Diebold's request, either due to the threat of an expensive lawsuit, or due to their Internet service provider/university refusing to risk a lawsuit, two students at Swarthmore College held their ground and filed an EFF assisted lawsuit. After the mainstream national and international press [NY Times, Guardian] picked up the story, Diebold backed down and retracted their DMCA requests, stating that "attempting to take further steps to enforce copyright interests when infringing material [had] proliferated across the Internet would not only be cost-prohibitive but in all likelihood futile" [Beacon].

John Halderman vs. SunnComm Technologies

In October 2003, John Halderman, a student of Dr Felten's, discovered that SunnComm Technologies' MediaMax CD-3 software, which is supposed to prevent some recent CDs from being copied by computers, could be disabled by users if they held the

shift key down as a protected CD was inserted into their computer. Soon after news of his research became public, the value of SunnComm's stock fell by 25 percent, equal to a loss of ten million dollars in market value. The company then announced that it "[intended] to refer this possible felony to authorities having jurisdiction over these matters because [...] the author's report was 'disseminated in a manner which facilitates infringement' in violation of the DMCA or other applicable law" [Register].

After being subjected to widespread ridicule in the technical [Wired 4] and national [NY Times 2] press and personally receiving three thousand criticizing emails, SunnComm's CEO Peter Jacobs announced that he had decided not to take legal action. "I don't want to represent a company that would do anything to cause any kind of chilling effect to research," Jacobs said. "Clearly the kind of emotional issues that surround this whole thing made it more prudent for us to take a step back and concentrate on making the next version better."

In addition to the previously described cases, there have been several other instances of companies quashing free speech and or legitimate research with DMCA cease and desist requests. These include: Hewlett-Packard attempting to silence researchers from revealing security flaws in their software [News.com], the church of Scientology forcing Google to remove anti-Scientology hyperlinks from their search engine [The Tan], and Microsoft threatening an MIT researcher for publishing security flaws in their X-Box gaming system [News.com 2].

The Stifling Effect on Legitimate Scientific Research

White House Cyber Security Chief Richard Clarke has called for DMCA reform due to its “chilling effect on vulnerability research” [Mercury] and has stated, “a lot of people didn’t realize that it would have this potential effect on vulnerability research” [Bray]. Fearing retribution from teams of DMCA wielding lawyers, some researchers have decided to stop publishing the results of their research, while others have resorted to performing their research in secret and then releasing their results anonymously. As the advancement of science depends upon peer review and an open atmosphere between researchers, this is having a devastating effect upon the academic community.

Niels Ferguson vs. the DMCA

In August 2001, Dutch cryptographer Niels Ferguson discovered a fatal flaw in the High-bandwidth Digital Content Protection (HDCP) system designed by Intel [Ferguson 1]. While Intel publicly stated they did not object to him publishing his paper [Ferguson 2], the possibility of prosecution by the US government or the movie studios, whose intellectual property would be protected by the HDCP system, gave him sufficient reason to not publish his research results.

In a statement to the court in the Felten case, he wrote that “The DMCA-risks to my personal liberty and financial security are simply too great. I am very angry at this restriction of my freedom of speech. I feel violated, helpless, and out of control. They have taken away a basic human right, and there is nothing I can do about it. Even publishing my paper here in the Netherlands will open the door to DMCA prosecution and liability. Not publishing this paper will damage my professional reputation, but if I do publish it I would never be able to visit the US again. This would do me even more

harm, both professionally and personally”, and that “Despite the fact that I performed all the work in Amsterdam, I could face arrest if I visit the US after my research had found its way into the jurisdiction. My research is silenced since I cannot talk about my scientific results to my colleagues and peers, as is now the case since the DMCA became law in the US. Scientific freedom is not only threatened under this law, it is demonstrably curtailed” [Ferguson 3].

Other Research Kept Quiet

There have been several other situations where researchers decided not to publish their results due to DMCA related fears. Dr Fred Cohen of University of New Haven removed his digital forensic analysis tool “Forensix” from his website [InfoSec], Dug Song, a highly regarded security expert and the author of several groundbreaking papers, took down his website and the several tools contained on it [Linux Sec] and an anonymous programmer who broke the encryption scheme protecting Microsoft’s electronic book format decided against publishing the source code to the exploit tool [I Anarchy].

Foreign Researchers Are Boycotting the U.S.

While some researchers are choosing to not publish their research or to publish it anonymously, some foreign researchers have chosen to stop traveling to the U.S. completely, fearing prosecution for “crimes” committed in their home countries when later traveling to the U.S. to speak at conferences.

In July 2001, Alan Cox, a widely respected Welsh programmer and the second most senior developer of the Linux operating system, announced that he would no longer travel to the U.S. for conferences, stating that “In my work on Linux security, I have to warn people about security problems I am aware of - indeed, for paid commercial work in the UK, failing to do so would almost certainly be negligent. Yet under the DMCA, I have to choose between keeping quiet when a flaw is known or discovered in an encryption system or other rights management tool, which could put my clients at risk -- or being unable to visit the United States without fear of arrest. Without that ability to tell the truth the fight against crime is weakened and the possibility that the national security infrastructure of nations is flawed and weak increases” [Cox]

In September 2001, responding to the arrest (and subsequent release) of a Russian programmer while visiting a conference in the US, the Russian Foreign Ministry issued a travel advisory, warning “all Russian specialists cooperating with U.S. firms in the computer software and programming business to the fact that [...] provisions of the [DMCA] may be used against them on U.S. territory” [NY Times 3].

Conclusion

While the DMCA may serve a legitimate purpose, it gives big businesses a powerful tool that they can and do use to intimidate researchers, students and those individuals acting for the public good. The US legal system puts those without deep pockets and a large team of lawyers at a significant disadvantage, which makes this a highly effective weapon in the arsenal of those companies wishing to crush any research that could cause negative press. This causes significant damage to the scientific

community, and in the case of Diebold's use of cease and desist letters, places the wellbeing of American democracy in danger. The lack of public information about security flaws places end users at risk, and ironically leaves copyright holders, those whom the DMCA was intended to protect, potentially exposed to mass theft due to unknowingly using flawed copy protection systems.

References

(in order of appearance)

- [UCLA]: UCLA Online Institute for Cyberspace Law and Policy, "The Digital Millennium Copyright Act," <<http://www.gseis.ucla.edu/iclp/dmca1.htm>> (Visited December 14 2003)
- [LOC]: US Library of Congress, "DMCA Summary," <<http://www.loc.gov/copyright/legislation/dmca.pdf>>
- [EFF 1]: The Electronic Frontier Foundation, "Unintended Consequences: Five Years under the DMCA," <http://www.eff.org/IP/DMCA/unintended_consequences.pdf> (Visited December 14 2003)
- [Frank]: Barney Frank, "House of Representatives - Congressional Record - August 4, 1998," <<http://www.house.gov/frank/digital98.html>> (Visited December 14 2003)
- [BTLJ]: Pamela Samuelson, "Intellectual Property and the Digital Economy," <<http://www.law.berkeley.edu/journals/btlj/articles/vol14/Samuelson/html/text.html>> (Visited Dec 14 2003)
- [ACM]: Barbara Simons and Eugene H. Spafford, Letter to the US Senate Subcommittee on Technology, Terrorism, and Government Information, <<http://www.acm.org/usacm/IP/dmca-feinstein-letter.html>> (Visited Dec 14 2003)
- [Mercury]: Jonathan Band, "Congress Unknowingly Undermines Cyber-Security," <<http://www.siliconvalley.com/mld/siliconvalley/4750224.htm>> (Visited December 15 2003)
- [Bray]: Hiawatha Bray, "Cyber Chief Speaks on Data Network Security," <<http://www.interesting-people.org/archives/interesting-people/200210/msg00063.html>> (Visited December 15 2003)
- [Cryptome]: Cryptome, "Felten v. RIAA history," <<http://cryptome.org/sdmi-attack.htm>> (Visited December 15 2003)
- [Felten 1]: Edward Felten, "Declaration of Edward Felten," <http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010813_felten_decl.html> (Visited December 15 2003)
- [Felten 2]: Electronic Frontier Foundation, "Security Researchers Drop Scientific Censorship Case," <http://www.eff.org/IP/DMCA/Felten_v_RIAA/20020206_eff_felten_pr.html> (Visited December 15 2003)
- [Anderson]: Ross Anderson, "Declaration of Ross Anderson," <http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011022_anderson_decl.pdf> (Visited December 15 2003)
- [Wired 1]: Kim Zetter, "Students Fight E-Vote Firm," <<http://www.wired.com/news/business/0,1367,60927,00.html>> (Visited December 15 2003)
- [Wired 2]: Kim Zetter, "Maryland: E-Voting passes muster," <<http://www.wired.com/news/business/0,1367,60583,00.html>> (Visited December 15 2003)

- [Rubin]: Avi Rubin, "Analysis of an Electronic Voting System,"
<<http://www.avirubin.com/vote/>> (Visited December 15 2003)
- [Wired 3]: Kim Zetter, "Diebold Backs Off Legal Challenge,"
<http://www.wired.com/news/evote/0,2645,61243,00.html>
(Visited December 15 2003)
- [Mercury 2]: AP Wire, "Diebold threatens publishers of leaked e-voting documents,"
<<http://www.siliconvalley.com/mld/siliconvalley/7117340.htm>> (Visited December 15 2003)
- [NY Times]: John Schwartz, "File Sharing Pits Copyright Against Free Speech,"
<<http://www.nytimes.com/2003/11/03/business/media/03secure.html>>
(Visited December 15 2003)
- [Guardian]: Rachel Konrad, "Electronic Voting Firm Sued Over Threats"
<<http://www.guardian.co.uk/uslatest/story/0,1282,-3349667,00.html>>
(Visited December 15 2003)
- [Beacon]: Erika D. Smith, "Diebold ends fight with online critics,"
<<http://www.ohio.com/mld/ohio/2003/12/02/business/7392949.htm>>
(Visited December 15 2003)
- [Wired 4]: Katie Dean, "Shift-Key Case Rouses DMCA Foes,"
<<http://www.wired.com/news/digiwood/0,1412,60780,00.html>>
(Visited December 15 2003)
- [NY Times 2]: Lisa Napoli, "Shift Key Opens Door to CD and Criticism,"
<<http://www.nytimes.com/2003/10/13/technology/13disk.html>>
(Visited December 15 2003)
- [Register]: Tony Smith, "SunnComm to sue 'shift key' student for \$10m",
<<http://www.theregister.co.uk/content/6/33322.html>>
(Visited December 15 2003)
- [News.com]: Declan McCullagh, "Security Warning Draws DMCA Threat,"
<<http://news.com.com/2100-1023-947325.html>>
(Visited December 15 2003)
- [The Tan]: Operation Clambake, "Scientologists gag Google,"
<<http://www.operatingthetan.com/google/ahl.txt>>
(Visited December 15 2003)
- [News.com 2]: David Becker, "Testing Microsoft and the DMCA,"
<<http://news.com.com/2008-1082-996787.html>>
(Visited December 15 2003)
- [Ferguson1]: Niels Ferguson, "Why I don't publish my HDCP results,"
<<http://macfergus.com/niels/dmca/cia.html>> (Visited December 15 2003)
- [Ferguson 2]: Niels Ferguson, "FAQ about DMCA and my HDCP paper,"
<<http://macfergus.com/niels/dmca/faq.html>> (Visited December 15 2003)
- [Ferguson 3]: Niels Ferguson, "Declaration of Niels Ferguson,"
<http://macfergus.com/niels/dmca/felten_declaration.html> (Visited December 15 2003)
- [InfoSec]: SWD Staff, "DMCA Fear Behind Info Evaporation,"
<<http://infosecuritymag.techtarget.com/2001/sep/digest10.shtml#news3>>
(Visited December 15 2003)

- [Linux Sec]: Ryan W. Maple, "Dug Song censors website, cites DMCA,"
<http://www.linuxsecurity.com/articles/cryptography_article-3624.html>
(Visited December 15 2003)
- [I Anarchy]: Erik Möller, "Microsoft E-Book Protection Cracked, Research
Unpublished,"
<<http://www.infoanarchy.org/story/2001/8/30/15248/3688>>
(Visited December 15 2003)
- [Cox]: Alan Cox, "Declaration of Alan Cox,"
<http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_cox_decl.htm>
(Visited December 15 2003)
- [NY Times 3]: John Jennifer Lee, "Travel Advisory for Russian Programmers,"
<<http://www.nytimes.com/2001/09/10/technology/10WARN.html>>
(Visited December 15 2003)