THINKPIECE

A CRITIQUE OF THE DIGITAL MILLENIUM COPYRIGHT ACT'S EXEMPTION ON ENCRYPTION RESEARCH: IS THE EXEMPTION TOO NARROW?

VICKY KU [*]

I. INTRODUCTION 466
II. PART I: WHAT IS ENCRYPTION RESEARCH? A BRIEF HISTORY 470
III. PART II: OVERVIEW OF SECTION 1201(A)(1) OF THE DMCA 474
A. WHAT DOES IT SAY? 474
B. WHAT WAS ITS INTENDED PURPOSE? 474
C. WHAT IS THE PURPOSE OF 1201(G)? 475
IV. PART III: IMPACT OF SECTION 1201(G) OF THE DMCA ON ENCRYPTION RESEARCH 485
A. WHO IN THE ACADEMIC COMMUNITY HAS BEEN AFFECTED? 485
V. PART IV: PROPOSED CHANGES TO THE DMCA 488
VI. CONCLUSION 489

Jointly reviewed and edited by Yale Journal of Law & Technology and International Journal of Communications Law & Policy.

[*] Author's Note.

A CRITIQUE OF THE DIGITAL MILLENIUM COPYRIGHT ACT'S EXEMPTION ON ENCRYPTION RESEARCH: IS THE EXEMPTION TOO NARROW?

VICKY KU *

Section 1201(g) of the Digital Millennium Copyright Act (DMCA) is offered as an exemption for encryption research.[1] However, the drafting of the exemption contradicts the purpose of copyright legislation under the terms of the Constitution, which is based upon the idea that the welfare of the public will be served and "to promote the progress of science and useful arts..."[2]

I. INTRODUCTION

On September 6, 2000, the Secure Digital Music Initiative (SDMI) issued the following invitation to the digital community, "Attack the proposed technologies. Crack them."[3] The challenge

---

Jointly reviewed and edited by Yale Journal of Law & Technology and International Journal of Communications Law & Policy.

* I would like to express my gratitude to Professor Richard Neumann for his constant guidance throughout the development of this paper, and law school in general. Also, many thanks go to my family. Without their encouragement and support, law school would not have been possible. For comments on the note, please contact the author at vku929@yahoo.com.

1 Digital Millennium Copyright Act, 17 U.S.C. §§ 1201-1205 (2003).

2 U.S. CONST. art. I, § 8, cl. 8.

3 Leonardo Chiariglione, *An Open Letter to the Digital Community*, SDMI, (Sept 6, 2000), *at* http://www.sdmi.org/pr/OL_Sept_6_2000.htm (last visited Mar. 29, 2005).http://www.sdmi.org/pr/OL_Sept_6_2000.htm (SDMI is a forum that has brought together more than 200 companies and organizations representing information technology, consumer electronics, security technology, the worldwide recording industry, and Internet service providers. SDMI's purpose was to develop technologies that protected "the playing, storing, and

was issued to the digital community as an "invitation to show off your skills."[4] To participate in the challenge, participants were directed to http://www.hacksdmi.org, a separate website created by SDMI, which detailed the terms and rules of the challenge.[5] Here, interested parties were required to read and agree to the public challenge agreement before they could participate.[6] The challenge offered compensation of $10,000 to anyone who "submitted a successful, unique attack on any individual technology" during the three weeks the SDMI Public Challenge was scheduled to run.[7] Edward Felten, a professor of

---

distributing of digital music such that a new market for digital music may emerge. However, based on its evaluation and testing of existing technology protection of digital music, it has determined that there is not yet consensus for adoption of any combination of the proposed technologies. As of May 18, 2001 SDMI is on hiatus, and intends to re-assess technological advances at some later date).

4 *Id.* (in issuing the challenge, SDMI explicitly acknowledged the value the digital community could provide in this type of exercise. The challenge stated in part that "the proposed technologies must pass several stringent tests: they must be inaudible, robust, and run efficiently on various platforms, including PCs. They should also be tested by *you*. By successfully breaking the SDMI protected content, you will play a role in determining what technology SDMI will adopt").

5 Complaint For Declaratory Judgment. and Injunctive Relief at ¶ 25, Felten v. RIAA, (No. CV-01-2669), *at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html (last visited Mar. 29, 2005).

6 *Id.* at ¶ 26-27.

7 *Id.* at ¶ 32. The Click-Through Agreement stated in part: "In exchange for such compensation, all information you submit, and any intellectual property in such information…will become the property of the SDMI Foundation and/or the proponent of that technology. In order to receive compensation, you will be required to enter into a separate agreement…. The agreement will provide that (1) you will not be permitted to disclose any information about the details of the attack to any other party…. *You may, of course, elect* not to receive compensation, in which event you will not be required to sign a separate document or assign any of your intellectual property rights, although you are still encouraged to submit the details of your attack.")(Emphasis added).

Computer Science at Princeton University, and a team of researchers at Princeton and Rice University, took on the challenge and succeeded in removing the encryption technologies that were in place.[8] Soon thereafter, Felten and the team decided to write a paper detailing their research and to submit the paper for publication to the Fourth International Information Hiding Workshop (IHW).[9] The paper was was submitted in late November 2000 and was put through a demanding peer review process.[10] In February 2001, Felten and his team were notified that their paper had been accepted for presentation at the conference on April 26, 2001.[11] On April 9, 2001, Felten received a letter from Matthew Oppenheim, Senior Vice President of Business and Legal Affairs of the Recording Industry Association of America, which expressed concern that the paper contained sensitive information about various technologies in the challenge that were copyrighted.[12] The letter stated in part that "disclosure...could result in significantly broader consequences and could directly lead to the illegal distribution of copyrighted material. Such disclosure...would subject your research team to enforcement actions under the DMCA and possibly other federal laws."[13]

---

8 *Id.* at ¶ 37.

9 *Id.* at ¶ 37; *see also* 6th Information Hiding Workshop, *at* http://msrcmt.research.microsoft.com/IH2004/CallForPapers.aspx (last visited Mar. 29, 2005). (The IHW is a peer-reviewed scientific conference that looks for papers covering topics such as anonymous communication, anonymous online transactions, privacy, and covert/subliminal communications, along with our usual quality watermarking and fingerprinting submissions.)

10 *Id.* at ¶ 38-39.

11 *Id.* at ¶ 38.

12 *Id.* at ¶ 42.

13 *Id.* at ¶ 43. The main issue was that the Challenge involved specific technologies that SDMI wanted tested, to see if they were vulnerable to attacks. One of these technologies, developed by Verance Corporation, was an audio watermarking solution designed to protect, manage and monitor audio and visual content. Verance objected to the paper because they felt that it provided unnecessarily detailed information, in particular relating to detailed numerical measurements" (such as frequencies and numeric parameters) that they felt did not

After much discussion regarding the threat of litigation against them, Felten and the research team decided to withdraw their paper from the IHW conference.[14] The research team cited as their primary reason for withdrawing the paper the fear of having to defend a lawsuit.[15] Ultimately, because Felten and his team were still interested in submitting their paper, they decided they would seek a declaratory judgement action in order to freely publish the paper.[16] On November 28, 2001, the Federal District Court in Trenton, New Jersey dismissed their case against the Recording Industry Association of America (RIAA) and the Department of Justice (DOJ).[17] Although Felten and the research team initially decided to appeal the Court's ruling, on February 6, 2002, they decided not to go forward with the appeal, in part due to assurances by the DOJ in their brief filed with the court that "scientists attempting to study access control technologies" are not subject to the Digital Millennium Copyright Act (DMCA).[18] The RIAA also stated that, "we felt Felten should publish his findings, because everyone benefits from research into the vulnerabilities of security mechanisms."[19] With this action, the DMCA discouraged copyrighted information from being disseminated. But did the DMCA do more harm than good?

This note analyzes section 1201(g), the encryption research exemption of the Digital Millennium Copyright Act and how the section as currently written has actually served to chill encryption research. Part I of this note provides a very brief history into encryption research and cryptography. Part II analyzes each provision within section 1201(g) to determine whether the provisions, as currently stated, further or inhibit

---

advance any "stated goals of furthering the academic body of knowledge).

14 *Id.* at ¶ 49.

15 *Id.* at ¶ 49.

16 *Id.* at ¶ 50.

17 Electronic Frontier Foundation, *Judge Denies Scientists' Free Speech Rights*, (Nov. 28, 2001, *at* http://www.eff.org/effector/HTML/effect14.37.html (last visited Mar. 29, 2005).

18 Electronic Frontier Foundation, *Security Researchers Drop Scientific Censorship Case,* Feb. 6, 2002, *at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20020206_eff_felten_pr.html, (last visited Mar. 29, 2005).

19 *Id.*

the "progress of science and the useful arts" which the Constitution states as one of the primary goals of Copyright laws. Part III highlights specific instances where the DMCA has been used to chill encryption research. Part IV looks at the future of the DMCA and how it will be used.

II. PART I: WHAT IS ENCRYPTION RESEARCH? A BRIEF HISTORY

Section 1201(g)(A) and (B) offer definitions for encryption research and technology:

> the term "**encryption research**" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and the term "**encryption technology**" means the scrambling and descrambling of information using mathematical formulas or algorithms.[20]

Although people tend to think of encryption as a relatively new phenomenon that only exists in the computer or technological world, encryption is simply another form of cryptography, which is defined as "the process or skill of communicating in or deciphering secret writings or ciphers."[21] The use of cryptography can be traced back to the earliest development of languages. It is probably not a stretch to say that from the moment man began to develop languages and to write things down, he also began to use codes to prevent others from deciphering what he had written; and of course, where there is a code, there is always someone who wants to break it. From Egyptian Hieroglyphics to the Underground Railroad to the Enigma machine in World War II and beyond, history provides many examples of successful and unsuccessful encryption "technologies."[22]

---

20 *See* 17 U.S.C. § 1201(g)(A) -(B).

21 THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (4th ed. 2000).

22 DAVID KAHN, THE CODEBREAKERS 71 (1967). In the 1900 B.C. a scribe's use of non-standard Egyptian hieroglyphs is

Modern encryption research dates back to 1976, when IBM Research developed the Data Encryption Standard (DES) block cipher cryptography.[23] DES is a widely used method of

---

documented as the first example of written cryptography); *see also* National Security Agency, *Historical Publications*, *at* http://www.nsa.gov/history/histo00007.cfm (last visited Mar. 29, 2005) (the Underground Railroad first began in 1780 to aid those who sought to escape slavery. In order for the Underground Railroad to work effectively, it was necessary to relay information to those attempting to make the trip to freedom. Because direct communication was not an option, the principals involved created a system based on designs sewn into quilts that could be conspicuously displayed in appropriate places. The quilts appeared as commonplace items to the adversaries of fugitive slaves. However, to those in flight, the quilts were symbols that advised them of the who, what, when, and how of their journey to freedom. Many of the symbols sewn into the patterns are obvious in their meanings, such as the monkey wrench, which denoted that it was time to gather the tools required to make the journey, or sailboats, which indicated the availability of boats for the crossing of crucial bodies of water. Other symbols were more cryptic, such as the star pattern, which had several variations but whose purpose was to point to the North Star. The Drunkard's Path pattern served to remind those on the run to move east to west (in much the way a drunken man staggers) during their journey. In short, the quilts were an invaluable aid in finding safe houses and in providing instructions, warnings, or reminders to those who were desperately trying to avoid capture), *see also* Enigma: History of Solving, *at* http://www.enigmahistory.org (last visited Mar. 29, 2005) (the German Enigma machine is one of the better known of the World War II cipher machines used by either side in the conflict. Invented in 1918, it was initially developed as a commercial cipher system, but although it failed commercially, it became the cryptographic workhorse of Nazi Germany. Enigma is an electro-mechanical device that utilizes a stepping wheel system to 'scramble' a plaintext message. Potentially, the number of cipher text alphabets is astronomically large - a fact that led the German military authorities to believe, wrongly as it turned out, in the absolute security of this cipher system).

23 IBM, *Research History Highlights*, *at* http://www.research.ibm.com/about/top_innovations_history.shtml (last visited Mar. 29, 2005).

data encryption using a private key that was judged so difficult to break by the U.S. government that it was adopted as a federal standard in 1977.[24] Although DES has served as the cryptographic standard for twenty-five years, and is still widely used by financial services and other industries, there are growing concerns about its vulnerabilities.[25]

With the current expansion of the Internet, computer security and encryption research issues have become increasingly more important. However, when one discusses computers, security and circumventing security, the image that comes to mind is that of the hacker – a geeky, young man locked in a basement busily trying to steal your credit card information. But not all cryptography or encryption research is done by hackers or computer geeks. In fact the National Security Agency (NSA) is "America's cryptologic organization."[26] The NSA "coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information."[27] As the Country's premier employer of codemakers and codebreakers, the NSA "is said to

---

24 *Id.*

25 RSA Security, *Press Releases: RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation (EFF)*, Jan. 19, 1999, *at* http://www.rsasecurity.com/company/news/releases/pr.asp?doc_id=462 (last visited Mar. 29, 2005) (at RSA Data Security's DES Challenge III, a secret message encrypted with the United States government's Data Encryption Standard (DES) algorithm was cracked in 22 hours and 15 minutes. Although DES was cracked, it is important to keep in mind that this was accomplished on a specially designed supercomputer, and a worldwide network of nearly 100,000 PCs on the Internet. RSA's original DES Challenge was launched in January 1997. The secret key was recovered in 96 days. Since that time, improved technology has made much faster exhaustive search efforts possible. DES Challenge II-1 was completed in 41 days and DES Challenge II-2 was cracked in 56 hours. The message to take away from these challenges is that DES may no longer be a viable encryption standard).

26 National Security Agency, *About the National Security Agency*, *at* http://www.nsa.gov/about/index.cfm (last visited Mar. 29, 2005).

27 *Id.*

be the largest employer of mathematicians in the United States and perhaps the world."[28]

In recent years it seems that the United States government has reluctantly come to realize the value of "hacking and hackers." In April 2002, the Government held the Cyber-Defense Exercise, which was designed to simulate a cyber-attack in a mock military network run by students of the Naval Postgraduate School.[29] The four-day event challenged student teams against professional military teams.[30] Although hardening the Nation's Internet defenses against cyber-attack has long been a goal of the government, the results have been slow in coming.[31] In 1999, the Clinton Administration drafted the National Plan for Critical Infrastructure and released it for public comment in 2000.[32] The plan detailed the steps the government should take in the event of an attack, to defend important national infrastructure, including communications and the Internet[33] "While the Cyber-Defense Exercise was not part of the National Plan, it does address one of the plan's ten steps: to train more security professionals."[34]

---

28 *Id.* (its mathematicians contribute directly to the two missions of the Agency: designing cipher systems that will protect the integrity of U.S. information systems and searching for weaknesses in adversaries' systems and codes).

29 Robert Lemos, *Training the cyberwar troops*, CNET NEWS.COM (Apr. 26, 2002), *at* http://zdnet.com.com/2100-1105-893418.html.

30 *Id.* (the blue teams were made up of students from the Naval Postgraduate School and other schools, while the red teams are made up of government employees from the National Security Agency and soldiers from the U.S. Air Force's 92nd Information Warfare Aggressor Squadron and the Army's Land Information Warfare Activity).

31 *Id.*

32 *Id.*

33 *Id.*

34 *Id.* (after last year's exercise, some students who participated in the exercise went to DefCon, the United States' largest hacker convention, to take part in the annual capture-the-flag tournament. The group went on the offensive for the showdown, in which teams of hackers attempt to compromise key servers on a mock network).

III. PART II: OVERVIEW OF SECTION 1201(A)(1) OF THE DMCA

A. WHAT DOES IT SAY?

The Digital Millennium Copyright Act (DMCA) was signed into law by President Clinton on October 28, 1998.[35] Congress enacted the DMCA as part of an effort "to begin updating national laws for the digital era."[36] The DMCA was designed to "facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age."[37] The DMCA sought to advance two goals: "the protection of intellectual property rights in today's digital environment and the promotion of continuing growth and development of electronic commerce."[38] The DMCA is divided into five components, but for the purposes of this note, we focus primarily on Section 1201(g) and sections related to encryption research.

B. WHAT WAS ITS INTENDED PURPOSE?

"No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[39]

Section 1201 of the DMCA was enacted with the purpose of providing adequate and effective protection against circumvention of technological measures used by copyright owners to protect their works.[40] To ensure that the public would have the ability to make fair use of copyrighted material, the DMCA was careful to distinguish between technological measures that prevent unauthorized access to a copyrighted work from those which prevent unauthorized copying of a copyrighted work.[41] Therefore, the act of circumventing a

---

35 Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

36 Copyright Office, *Report to Congress: Joint Study of Section 1201(g) of the Digital Millennium Copyright Act*, *at* http://www.copyright.gov/reports/studies/dmca_report.html (last visited Mar. 29, 2005).

37 *Id.*

38 *Id.*

39 17 U.S.C. § 1201(a)(1)(A).

40 *See, e.g.*, 17 U.S.C. § 1201(g)(5)(B).

41 COPYRIGHT OFFICE SUMMARY, REPORT ON THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998.

technological measure in order to gain access is prohibited.[42] The DMCA does allow for a few exceptions that include law enforcement activities, reverse engineering, and encryption research.[43] However, these exceptions are extremely narrow, and it is section 1201(g) – the exemption for encryption research -- that is analyzed below.

C. WHAT IS THE PURPOSE OF 1201(G)?

A simple reading of Section 1201(g) immediately raises a whole host of questions. In general, the exemption seems to create more problems than it proposes to solve. By breaking down the exemption, provision by provision, we can see ultimately how ineffective this section will be in actually preventing access to copyrighted materials.

Section 1201(g)(1) begins by offering definitions for encryption research and encryption technology. Section 1201(g)(2) lists the "permissible acts of encryption research."

> 1201(g)(2)Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if--
>
> 1201(g)(2)(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;
>
> 1201(g)(2)(B) such act is necessary to conduct such encryption research;

Analysis - Here the provisions are acceptable. There is no reason for a researcher who is conducting legitimate encryption research not to first lawfully obtain an encrypted copy of whatever it is that they are trying to decrypt. Furthermore, it is usually necessary to obtain a copy of the encrypted work to analyze it and decrypt it.

---

42 COPYRIGHT OFFICE SUMMARY, REPORT ON THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998.

43 17 U.S.C. § 1201(e), § 1201(f), and § 1201(g).

> 1201(g)(2)(C) the person made a good faith effort to obtain authorization before the circumvention;

Analysis – The problems begin with Section 1201(g)(2)(C), which provides that "the person make a good faith effort to obtain authorization before the circumvention." This provision obviously places an encryption researcher in somewhat of a dilemma. What constitutes "a good faith effort?" Does this mean the researcher should send a letter to the company, make a phone call, send an email? What would the researcher say? That he would like the company's authorization to discover flaws in their technology? What company would allow this? What if the researcher does attempt to contact the company and there is no reply? Should the researcher assume that the authorization has been denied and abandon the research? If the researcher makes a good faith attempt and is specifically denied, can he go ahead with his research? If so, does this defeat the requirement to seek authorization entirely? Based on the analysis above, this provision serves no useful purpose and is essentially meaningless as it is currently drafted.

> 1201(g)(3) Factors in Determining Exemption – In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—
>
> 1201(g)(3)(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;

Analysis – The main question here is what purpose does information derived from encryption research serve, if it is *not* disseminated? Why would a researcher seek to analyze any type of encryption research if they were not planning to disseminate their findings? Furthermore, what qualifies as dissemination? The statute seems to close off all possibilities for researchers while at the same time managing to seem magnanimous about allowing the research in the first place. If for example, a

researcher were to share his or her findings with a colleague then this would presumably fit within the scope of "disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology."[44] But what if the researcher decided to publish the information on a website? Perhaps he simply wants to share his findings with a broader audience, should he then be responsible for every single person that accesses the website and reads his research?

Take for example the recent problems surrounding John Halderman's publication of a significant weakness in encryption software developed by SunnComm Technologies.[45] On October 6, 2003, Halderman, a doctoral candidate at Princeton, published a study which detailed how the company's encryption software could be defeated by holding down the 'Shift' key.[46] The report was published on Halderman's personal website and in the Princeton University Computer Science Technical Report (October 2003).[47] Three days after the paper was published, SunnComm Technologies' chief executive officer, Peter Jacobs, threatened to sue Halderman for criminal violations of the DMCA.[48] After a barrage of negative press, Jacobs reversed his

---

44 17 U.S.C. § 1201(g)(3)(A).

45 *CD copy protection trumped by Shift key*, CNN.COM (Oct. 8, 2003), *available at* http://homepages.law.asu.edu/~dkarjala/cyberlaw/CopyProtectionTrumpedCNN-com10-8-03.htm (last visited Mar. 29, 2005).

46 John A. Halderman, Analysis of the MediaMax CD3 Copy-Prevention System, *at* http://www.cs.princeton.edu/~jhalderm/cd3/ (last visited Mar. 29, 2005).

47 *Id.*; *see also* John A. Halderman, *Analysis of the MediaMax CD3 Copy-Prevention System*, Princeton Univ. Computer Sci. Technical Reports, TR-679-03 (2003), *at* http://ncstrl.cs.princeton.edu/expand.php?id=TR-679-03 (last visited Mar. 29, 2005). – the font size needs to be fixed on this cite

48 Katie Dean, *Shift-Key Case Rouses DMCA Foes*, WIRED.COM (Oct. 11, 2003), *at* http://www.wired.com/news/digiwood/0,1412,60780,00.html; *see also* Press Release, SunnComm, SunnComm CEO Says Princeton Report Critical of its MediaMax CD Copy Management Technology Contains Erroneous Assumptions and Conclusions (Oct. 9, 2003), *at*

position and decided not to sue Halderman, stating, "I don't want to be the guy that creates any kind of chilling effect on research."[49] To have your adversary acknowledge that defending a lawsuit based on violations of the DMCA would create a chilling effect on research, is a pretty strong suggestion that it is true.

Although it may be stating the obvious, the fact is that the most valuable information involved in encryption research will most likely involve information on how to "crack" the code. This is precisely the type of information that is most useful to a researcher in this field. Essentially *any* publication or discussion of the weaknesses of a particular encryption tool could "*facilitate infringement...*"[50]

An interesting correlation to the problem of requiring researchers to control dissemination of information that facilitates infringement is the very recent storm of controversy created by the Motion Picture Association of America (MPAA). On September 30, 2003, Jack Valenti, President and CEO of the MPAA, announced that in an effort to "combat digital piracy and to save movie jobs in the future," certain movie studios would no longer provide screening copies for awards consideration purposes.[51] This announcement caused widespread criticism within the film industry, many of whom stated that the move would make it harder for smaller films to win Oscars.[52] In

---

http://www.sunncomm.com/press/pressrelease.asp?prid=200310091000 (last visited Mar. 29, 2005).

49 Josh Brodie, *Threat of lawsuit passes for student*, *at* THE DAILY PRINCETONIAN (Oct. 10, 2003), *available at* http://www.dailyprincetonian.com/archives/2003/10/10/news/8797.shtml; *see also* Katie Dean, *Shift-Key Case Rouses DMCA Foes*, WIRED.COM (Oct. 11, 2003), *at* http://www.wired.com/news/digiwood/0,1412,60780,00.html.

50 17 U.S.C. § 1201(g)(3)(A).

51 Press Release, Jack Valenti, Motion Picture Association of America, Film Studios Announce End To Award Screeners: Measure Taken To Combat Piracy (Sept. 30, 2003), *at* http://www.mpaa.org/jack/2003/2003_09_30aindex.htm (last visited Mar. 29, 2005.

52 David Germain, *Oscars ban 'screening' tapes*, THE ENQUIRER (Oct. 2, 2003), *at* http://www.enquirer.com/editions/2003/10/02/tem_1002oscars.html.

October, 2003, an open letter criticizing the screener ban was signed by over 140 directors, including Martin Scorsese, Francis Ford Coppola and Robert Redford.[53] On October 23, 2003, the MPAA partially reversed their position and stated that they would allow the "screener" copies but with certain exceptions.[54] Under the new agreement, Academy members would be required to sign a pledge that they would not allow the screener copy out of their home, or pass the screener to family or friends.[55] Furthermore, if a screener copy is pirated, the information can be traced back to the original source and the guilty member will face immediate expulsion from the Academy.[56] In effect, this new procedure operates in much the same way Section 1201(g)(3)(A) of the DMCA does, by requiring anyone who lawfully receives a screener copy to consider very carefully how they might be responsible for *disseminating or facilitating infringement*, even if they are simply loaning the screener copy to another Academy member. In response to the screener ban and the exceptions stated by the MPAA, the Los Angeles Film Critics Association called off its awards ceremony this year in protest.[57] Jean Oppenheimer, the group's president, said the awards cancellation will stand unless the MPAA rescinds the entire screener ban.[58] On November 5, 2003, the

---

53 Josh Grossberg, *Directors Diss Screener Ban*, EONLINE.COM (Oct. 10, 2003), *at* http://www.eonline.com/News/Items/0,1,12669,00.html.

54 Press Release, Jack Valenti, Motion Picture Association of America, Academy Announce Plan to Reinstitute Awards Screeners (Oct. 23, 2003), *at* http://www.mpaa.org/jack/2003/2003_10_23index.htm (last visited Mar. 29, 2005).

55 *Id.*

56 *Id.*

57 Josh Grossberg, *L.A. Critics Call Off Awards*, E! ONLINE (Oct. 20, 2003), *at* http://www.eonline.com/News/Items/0,1,12732,00.html (last visited Mar. 29, 2005).

58 Lia Haberman, *Oscar Screener Squabble Continues*, E! ONLINE (Nov. 7, 2003), *at* http://www.eonline.com/News/Items/0,1,12872,00.html. (last visited Mar. 29, 2005).

Chicago Film Critics Association announced that it would also suspend its awards ceremony due to the screener ban.[59]

Requiring encryption researchers to police the dissemination of their work is inherently illogical given that the type of research involved here is only valid when it is widely disseminated and can be frequently tested and challenged by other encryption researchers.

> 1201(g)(3)(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology [60]

Analysis – The provision possesses a number of serious deficiencies. The first part of the provision naturally begs the question, "what would the DMCA characterize as a legitimate course of study?" There is no definition provided in the DMCA itself. Does legitimate refer to only encryption research and cryptology backgrounds? But cryptology is a derivative of mathematics. What about the sciences, computer science, etc.? If you are a student like John Halderman, are you excluded from the exemption until you obtain a Ph.D.? The second part focuses on employment in the field of encryption. To what purpose does this serve? The field of encryption research is a small field already, to limit it further to only those currently employed in the field would eliminate those who can offer legitimate contributions but perhaps are employed in different fields. Moreover,, if a person decides to decrypt a given technology and obtains the software lawfully, why should it matter what industry or field of study they are employed in?

The last provision, which requires that the person be appropriately trained or experienced, places unnecessary and detrimental limitations to the exemption. "This is a fast-moving field and many of the most creative results have come from

---

59 *Id.*; *see also Judge Sacks Screener Ban*, CBSNEWS.COM (Dec. 5, 2003), *at* http://www.cbsnews.com/stories/2003/10/24/entertainment/main579885.shtml (last visited Mar. 29, 2005) (on December 5, 2003, a U.S. District Court judge granted a temporary restraining order against the ban, allowing screener tapes to be used. The MPAA has stated that they intend to appeal the decision).

60 17 U.S.C. § 1201(g)(3)(B).

individuals without formal training in cryptography."[61] "The information technology industry... has a rich tradition of individuals – often not associated with any corporation or organization, and often without any formal training – who seek to crack security implementations and publicly demonstrate their shortcomings." [62] "Some of the amateurs I know have been a vital resource that were [sic] crucial to some of my academic discoveries." [63] "An interesting aspect of today's research is that relative unknowns do some of the most important new work. [S]ome of the finest research today comes from groups of researchers... [who are] typically young, brash, [and] contemptuous of the authorities that created these security

---

61 Hal Finney, Network Associates, Inc., *at* http://www.copyright.gov/reports/studies/comments/003.pdf (July 12, 1999) (last visited Mar. 29, 2005) (Finney is a Senior Software Engineer at Network Associates. His comments were considered when drafting the NAT'L TELECOMM. INFO. ADMIN. & U.S. COPYRIGHT OFFICE, REPORT TO CONGRESS: JOINT STUDY OF SECTION 1201(g) OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, *available at* http://www.copyright.gov/reports/studies/dmca_report.html) (last visited Mar. 29, 2005).

62 Peter F. Harter, on behalf of Emusic.com, *at* http://www.copyright.gov/reports/studies/comments/010.pdf (July 26, 1999) (last visited Mar. 29, 2005) (Harter is the Vice President of Global Public Policy & Standards for EMusic.com. His comments were considered when drafting the NAT'L TELECOMM. INFO. ADMIN. & U.S. COPYRIGHT OFFICE, REPORT TO CONGRESS: JOINT STUDY OF SECTION 1201(g) OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, *available at* http://www.copyright.gov/reports/studies/dmca_report.html) (last visited Mar. 29, 2005).

63 David Wagner, University of California, Berkeley, *at* http://www.copyright.gov/reports/studies/comments/001.pdf (May 27, 1999)))) (last visited Mar. 29, 2005) (Wagner is an Assistant Professor in the Computer Science Division. His comments were considered when drafting the NAT'L TELECOMM. INFO. ADMIN. & U.S. COPYRIGHT OFFICE, REPORT TO CONGRESS: JOINT STUDY OF SECTION 1201(g) OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, *available at* http://www.copyright.gov/reports/studies/dmca_report.html) (last visited Mar. 29, 2005).

systems (often that contempt is well-placed)." [64] For many, this description brings to mind the quintessential image of the hacker. However, although the term hacker is now used pejoratively, it was initially a positive term, describing a person "who enjoys learning the details of computer systems and how to stretch their capabilities—as opposed to most users of computers, who prefer to learn only the minimum amount necessary," or "One who programs enthusiastically or who enjoys programming rather than just theorizing about programming".[65]

Ironically, many of the earliest hackers came from the best universities this country had to offer.[66] Additionally, hackers are credited with the development of a wide variety of

---

64 Jonathan D. Callas, Counterpane Internet Security, *at* http://www.copyright.gov/reports/studies/comments/012.pdf (July 26, 1999)))) (last visited Mar. 29, 2005) (Callas is a Senior Systems Architect at Counterpane. His comments were considered when drafting the NAT'L TELECOMM. INFO. ADMIN. & U.S. COPYRIGHT OFFICE, REPORT TO CONGRESS: JOINT STUDY OF SECTION 1201(g) OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, *available at* http://www.copyright.gov/reports/studies/dmca_report.html) (last visited Mar. 29, 2005).

65 E. S. Raymond, *The New Hacker's Dictionary*, MIT Press, Cambridge, MA (1991).

66 Erik Brunvand, *A Little Bit of Hacker History*, *at* http://www.cs.utah.edu/~elb/folklore/afs-paper/node3.html (Oct. 15, 1996) (last visited Mar. 29, 2005) (the early history of hackers is centered around MIT in the 1950's and 1960's. The mid 1960's saw centers of hacker culture develop at other universities such as Carnegie Mellon University, and Stanford University. The Stanford Artifical Intelligence Lab (SAIL), became the center for west-coast hacker activity. Even commercial research centers were home to hackers. AT&T, Xerox, and others all had programmers of legendary skill working for them. The third wave of hacker activity began in Northern California. This was a group of electronic hobbyists with a common interest in the then radical idea of building their own computers. This group of hackers, includes legendary figures such as Steve Wozniak, Steve Jobs, and Bill Gates, that formed the foundation for the entire personal computer industry).

technologies that are now considered to be standards within the computer industry.[67] If this provision of the DMCA were in place in the 1970s, there is no telling how many of these "hackers" would have been prevented from contributing their knowledge to the growth of the computer industry.

Even as the government prosecutes researchers under the DMCA, it is also adopting the attitude that "if you can't beat them, join them." Although this attitude comes more from necessity than from any real desire to engage the "hacker community," the reality is that what was once a niche group of hackers is now a respected and influential group of people that can provide a wealth of information and valuable skills to the area of technological and cyber security. In August of 2003, the DefCon conference held its annual "Capture the Flag" game that is known as Root Fu.[68] The purpose of the contest is to challenge teams at the conference to "play" against each other in a test of network defense and hacking skills.[69] "This sort of adversarial testing shows what is possible--and not--with security," said Crispin Cowan, chief scientist at Linux security seller Immunix and the leader of the Immunix team.[70] "We value this competition, because we think it is a better evaluation of security than common criteria."[71] Alan Harper, a security engineer with the Defense Information Systems Agency (DISA), thinks that competitions like Root Fu can help others understand that all hacking isn't bad.[72] Immunix's Cowan

---

67 The Learning Channel, *Hackers: A Brief History of Hacking*, *available at* http://tlc.discovery.com/convergence/hackers/articles/history.html (last visited Mar. 29, 2005) (maybe the best hack of all time was created in 1969, when two employees at Bell Labs' think tank came up with an open set of rules to run machines on the computer frontier. Dennis Ritchie and Ken Thompson called their new standard operating system UNIX. UNIX is now the most common operating system for servers on the Internet).

68 Robert Lemos, *Hacking Contest Promotes Security*, CNET NEWS.COM (Aug. 4, 2003), *at* http://news.com.com/2100-1009-5059827.html?tag=nl (last visited Mar. 29, 2005) (Root Fu is a hackerish name that is derived from a super user's name on UNIX systems, root, and the final syllable of kung fu).

69 *Id.*

70 *Id.*

71 *Id.*

72 *Id.*

further stated that exercises and security challenges like Root Fu may have settled a long-debated point: whether hackers make the best defenders.[73] "The offensive attackers have been doing the best code auditing. They attack, find the holes and then tell the defenders on the team."[74] The challenge highlights the fact that knowing how to attack systems is a critical skill in learning how to defend them.[75]

Ultimately, it is important to remember that the whole purpose of establishing this exemption in the DMCA was to open up the field to certain individuals, but when the exemption itself contains arbitrary limitations that serve no useful purpose, it defeats the validity of the exemption entirely.

> 1201(g)(3)(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.[76]

Analysis – The initial question is, Why? Why should a researcher have to provide the copyright owner with notice of their findings and documentation of their research? This factor simply serves to negate the effect of the provisions that came before it. Essentially, this factor says if you're going to do your research anyway, research that would provide a useful purpose, then you should give your findings to the corporation whose technology you have decrypted. The corporation did not want you to decrypt their software and they might still sue you but give them the research anyway, so that they can make improvements to their faulty software. Also, isn't disseminating it publicly still providing the copyright owner with notice? But this is not allowed, so essentially this factor is saying that only the copyright owner is entitled to the researcher's findings.

---

73 *Id.*
74 *Id.*
75 *Id.*
76 17 U.S.C. § 1201(g)(3)(C).

IV. PART III: IMPACT OF SECTION 1201(G) OF THE DMCA ON ENCRYPTION RESEARCH

A. WHO IN THE ACADEMIC COMMUNITY HAS BEEN AFFECTED?

In addition to the problems that Edward Felten and his research team faced with the SDMI challenge and the recent problems John Halderman faced, there are other examples of how encryption around the world has been affected. In May 1999, six months after Congress first enacted the DMCA, the Copyright Office and the National Telecommunications and Information Administration (NTIA) issued a joint Federal Register notice soliciting public comment on the effects of Section 1201(g) of the DMCA.[77] The report that followed a year after offered a brief view of the legislative background of Section 1201(g) and summarized the substance of the public comments received by the Copyright Office and NTIA.[78] The report highlighted the substantive portions of the comments which focused specifically on Sections 1201(g)(2)(C) and 12(g)(3) and all its relevant parts and disingenuously concluded that because there was currently no specific evidence of the DMCA having a negative impact on encryption research, there would be no need to alter or change the language of the pertinent sections.[79] The report stressed that because the

---

77 Request for Comments on Section 1201(g) of the Digital Millennium Copyright Act, 64 Fed. Reg. 28, 802 (Dep't Commerce May 27, 1999), *available at* http://www.copyright.gov/fedreg/1999/64fr28802.pdf (last visited Mar. 29, 2005).

78 NAT'L TELECOMM. INFO. ADMIN. & U.S. COPYRIGHT OFFICE, REPORT TO CONGRESS: JOINT STUDY OF SECTION 1201(g) OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, *available at* http://www.copyright.gov/reports/studies/dmca_report.html)(comments were received from both proponents (TimeWarner, Software & Information Industry Association (SIIA) and the American Society of Composers, Authors and Publishers (ASCAP) and opponents of the DMCA (EMusic.com and several notable encryption researchers).

79 *Id.* ("Of the 13 comments received in response to the Copyright Office's and NTIA's solicitation, not one identified a *current, discernable impact on encryption research* and the development of encryption technology")(Emphasis added).

exceptions would not become operative until October 28, 2000, that any changes would be "entirely speculative…and premature." [80] In April 2001, just six months after the DMCA exceptions went into effect, SDMI and Verance Corporation would threaten to sue Edward Felten and his research team for copyright infringement under the DMCA.[81]

On July 16, 2001, the FBI arrested Russian encryption expert, Dmitry Sklyarov, an employee for ElcomSoft Co., for criminal violations of the DMCA. [82] Sklyarov was arrested at his hotel in Las Vegas, after he had spoken at the DefCon hacking conference, where he outlined the problems plaguing e-book formats and Adobe's PDF format.[83] If convicted, Sklyarov would have faced a maximum penalty of a $500,000 fine and five years in prison.[84] Although the criminal charges against Sklyarov were later dropped, ElcomSoft was charged with developing and distributing a software program that allowed users to circumvent the copyright protection in Adobe Systems' e-book file format.[85] A year and a half after the initial charges,

---

80 *Id.*

81 *See* Felten, *supra* note 5, at ¶ 42.

82 Robert Lemos, *Russian Crypto Expert Arrested at Def Con*, CNET NEWS.COM (July 17, 2001), *at* http://news.com.com/2100-1001-270082.html?legacy=cnet.

83 *Id.* DEF CON is an annual computer underground party for hackers held in Las Vegas, Nevada. It is currently in its eleventh year with over 5000 in attendance, making it one of the largest hacking conventions in the world. Ironically, the day before Sklyarov was arrested, a seven-member panel called "Meet the Feds" was held. The panel of government officials, members of law enforcement, a congressman and security experts, was designed to illuminate the problems the government has faced in securing systems and also to appeal to hackers to work together and not against each other.

84 *Id.*

85 Scarlet Pruitt, *Copy Control Case Hits Court*, PC WORLD.COM (Dec. 2, 2002), *at* http://www.pcworld.com/news/article/0,aid,107514,00.asp (the software allowed users to disable security settings on Adobe Systems' e-book files so they could be printed, shared, and viewed on various computing devices).

the case went to court and a jury delivered a verdict of not guilty and absolved ElcomSoft of all charges.[86]

In August 2001, Niels Ferguson, a professional cryptographer from the Netherlands, posted on his website an announcement that he had discovered significant security weaknesses in the High-bandwidth Digital Content Protection (HDCP) cryptographic system developed by Intel.[87] Ferguson stated that "HDCP is fatally flawed," and that "[t]he flaws in HDCP are not hard to find.[88] As I like to say: 'I was just reading it and it broke.'"[89] Although he has written a paper detailing the weaknesses in HDCP, he stated that he would not publish his results for fear of prosecution under the DMCA.[90]

Proponents of the DMCA are quick to point out that the reaction from encryption researchers is extreme and unnecessarily dramatic. Allan Adler, vice president of the Association of American Publishers (AAP) blames organizations like the Electronic Frontier Foundation, which represented Edward Felten in his suit against the RIAA, for dramatizing the negative effects of the DMCA.[91] "They succeeded in creating a kind of chilling effect in the scientific community because of the

---

86 Matt Berger, *Verdict Delivers Blow to the DMCA*, PC WORLD.COM (Dec. 17, 2002), *at* http://www.pcworld.com/news/article/0,aid,108040,00.asp.

87 Niels Ferguson, *Censorship in Action: Why I don't Publish My HDCP Results*, *at* http://macfergus.com/niels/dmca/cia.html (last visited Mar. 29, 2005) (Ferguson is a cryptographic engineer and consultant at Counterpane Internet Security (CIS). He has extensive experience in the design and implementation of cryptographic protocols and large-scale security infrastructures. He has published numerous scientific papers and co-authored a book with the founder of CIS, Bruce Schneier, called *Practical Cryptography*. HDCP is used to prevent illegal copying of video contents by encrypting the signal). font size is wrong in this cite

88 *Id.*

89 *Id.*

90 *Id.* ("I have been advised by a US lawyer who works in this field that if I publish my paper, I might very well be prosecuted and/or sued under US law.").

91 Declan McCullagh, *Debunking DMCA Myths*, CNET NEWS.COM (Aug. 19, 2002), *at* http://news.com.com/2010-12-950229.html.

kind of fear-mongering they were engaged in."[92] Orin Kerr, a law professor at George Washington University and a former prosecutor for the Justice Department, stated that "[o]pponents of the DMCA want to dramatize its effects, so they want people to believe that the law is incredibly broad."[93] However, the Electronic Frontier Foundation argues that "Not every grad student or even professor is going to have easy access to free counsel who can provide a counterweight to the university lawyers."[94]

V. PART IV: PROPOSED CHANGES TO THE DMCA

In January 2003, Rep. Rick Boucher, D-Va., reintroduced a bill he first unveiled late last year that aims to protect consumers and legitimate researchers by carving out more protections for them in the DMCA.[95] Mr. Boucher, a longtime critic of the DMCA, says, "The fair use doctrine is threatened today as never before. The reintroduced legislation will assure that consumers who purchase digital media can enjoy a broad range of uses of the media for their own convenience in a way that does not infringe the copyright in the work."[96] Supporters of the latest version of the bill are said to include Intel, Verizon, Sun Microsystems, Gateway, and the Consumer Electronics Association.[97] Richard Clarke, Special Adviser for Cyberspace Security within the National Security Council, has also called for amendments to the DMCA because of its ``chilling effect on vulnerability research."[98] "Personally, I think the answer to

---

92 *Id.*

93 *Id.*

94 *Id.*

95 Digital Media Consumers' Rights Act of 2003, H.R.107, 108th Cong. (2003). *See also* Lisa M. Bowman, *Norway Piracy Case Brings Activists Hope*, CNET NEWS.COM (Jan 8, 2003), *at* http://news.com.com/2100-1023-979769.html.

96 Bowman, *supra* note 95.

97 *Id.*

98 Jonathan Band, *Congress Unknowingly Undermines Cyber-security*, SILICON VALLEY (Dec. 16, 2002), *at* http://www.siliconvalley.com/mld/siliconvalley/4750224.htm

that is yes. We need to have everyone in this country who's an IT expert looking for vulnerabilities."[99]

VI. CONCLUSION

The question comes down to, "What are we protecting?" The technology, the intellectual property behind the technology, or the "freedom to tinker?"[100] If a CD or movie is protected by a software that can be disabled, circumvented or cracked by teenagers, can it still be considered a viable form of protection?

Although the most visible aspect of the controversy surrounding encryption research involves intellectual property and copyright protections, the issue is much larger than just protecting music from being illegally downloaded. Encryption research plays a large role in our government defense systems, in the move towards online voting, and in the growth and security of the Internet itself. While speaking at a conference at the Massachusetts Institute of Technology, former White House counter-terrorism advisor Richard Clarke stated that "[s]omebody, someday is going to hurt our economy if we don't start dealing with our vulnerabilities." .[101]

Whom does the DMCA actually target? Why should it matter if a software is flawed and a researcher discovers this, publishes his findings and is later prosecuted? At this point, the

---

99 Dennis Fisher, *Clarke Solicits IT Security at MIT* EWEEK (Oct. 17, 2002) *at* http://www.eweek.com/article2/0,1759,639096,00.asp.

100 Ed Felten, *Freedom to Tinker*, *at* http://www.freedom-to-tinker.com (last visited Dec. 15, 2003); *see also* Abusable Technologies Awareness Center (ATAC), *at* http://www.abusabletech.org/ (whose mission is to "provide current and accurate information about technology that oversteps its bounds. Whether the concerns relate to unexpected privacy violations or inappropriate security, ATAC serves as a clearinghouse for informed discussions." This new weblog is made up of respected computer scientists and hosted by the Information Security Institute at Johns Hopkins University)(last visited Sept. 15, 2004).

101 Dennis Fisher, *Clarke Solicits Cyber-Security Input at MIT*, EWEEK.COM (Oct. 17, 2002), *at* http://www.eweek.com/article2/0,3959,639096,00.asp.

DMCA has not prevented those that can crack a given technology to stop doing it; the DMCA has simply encouraged them to keep quiet about it. On the other hand, the DMCA offers valuable protection to companies that claim their software is secure when it is not. Peter Harter, Vice President of EMusic, an online song-sharing company, stated that "proponents of industry standards can use (the DMCA) to squelch legitimate criticism and analysis of those standards, including criticism and analysis that is not in the least bit motivated by a desire to gain unauthorized access to copyrighted works."[102]

As Niels Ferguson states on his website, to potential customers who wish to hire him, "Cryptography looks deceptively easy...But bad cryptography looks just like good cryptography. There is no way to tell them apart from the outside...until the system is attacked. There is no point in using cryptography if it is not done well. Bad cryptography is just as expensive as good cryptography, but it is completely ineffective."[103] Ultimately, Section 1201(g) of the DMCA does nothing to further the "welfare of the public" or "promote the progress of science and useful arts."[104]

---

102 Lisa M. Bowman, *Hacker Arrest May Spur Review of Digital Rules*, CNET NEWS.COM (July 27, 2001), *at* http://news.com.com/2100-1023_3-270728.html?tag=st_rn.

103 Niels Ferguson, *MacFergus Services*, *at* http://macfergus.com/services.html (last visited Sept. 15, 2004).

104 U.S. CONST. art. I, § 8, cl. 8.