

THE DMCA AND THE REGULATION OF SCIENTIFIC RESEARCH

By Joseph P. Liu[†]

ABSTRACT

This Article analyzes the impact of the Digital Millennium Copyright Act (DMCA) on academic encryption research. In this Article, I argue that for both legal and practical reasons academic encryption researchers should be able to conduct and publish certain types of research without significant fear of liability under the DMCA. However, the DMCA will have a non-trivial impact on the conditions under which such research takes place, and this impact can be expected to have several undesirable effects. More broadly, this impact highlights the problematic way in which the DMCA regulates scientific research in furtherance of intellectual property rights. The Article concludes with a number of suggestions for mitigating some of these negative effects.

TABLE OF CONTENTS

I.	INTRODUCTION	502
II.	BACKGROUND ON THE DMCA AND ENCRYPTION RESEARCH	505
A.	The DMCA and the Encryption Research Exemption	505
B.	Criticism of the DMCA and the Exemption	509
C.	Initial Cases Implicating the Exemption	513
D.	Responses by Encryption Researchers	514
III.	IMPACT OF THE DMCA ON ENCRYPTION RESEARCH	517
A.	Academic Encryption Research Can Still Take Place	517
B.	The DMCA Affects the Manner in Which Research Is Conducted	523
IV.	A NORMATIVE ASSESSMENT OF THE DMCA'S IMPACT	528
V.	POTENTIAL LEGAL RESPONSES	535
VI.	CONCLUSION	537

© 2003 Joseph P. Liu

† Assistant Professor, Boston College Law School. Thanks to Hal Abelson, Stacey Dogan, Dean Hashimoto, Andrew “bunnie” Huang, Pamela Samuelson, Lee Tien, Fred Yen, and the participants at the Second Annual Intellectual Property Scholars Conference at Cardozo Law School, for helpful comments and suggestions. Thanks also to Anderson Kizzie for research assistance. I should disclose at the outset that I have worked with the Electronic Frontier Foundation (EFF) on a number of cases involving the application of the DMCA to encryption research. See, e.g., Compl. Declaratory J. and Injunctive Relief, Felten v. Recording Indus. Ass’n (RIAA) (D.N.J. Nov. 28, 2001) (No. CV-01-2669), available at http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_com_complaint.html. The views expressed in this Article, however, are solely mine and do not represent the views of the EFF or any other organization.

I. INTRODUCTION

The Digital Millennium Copyright Act of 1998 (DMCA)¹ has been the subject of significant controversy. In particular, the anti-circumvention provisions of the DMCA²—the provisions that impose liability for circumventing technological measures used to protect copyrighted works—have been the target of much criticism from academics, consumer groups, and civil libertarians.³ DMCA critics have argued that these provisions unduly shift the preexisting balance of interests in copyright law toward copyright holders and away from copyright consumers and the public at large.⁴ At the same time, supporters of the DMCA, including members of the movie and music industries, have vigorously defended these provisions, arguing that they are necessary to prevent unauthorized copying of copyrighted works in the digital environment.⁵

My purpose in this Article is not to address, at least directly, the broader debate over the wisdom or propriety of the DMCA's anti-circumvention provisions. Instead, this Article focuses on a much narrower issue: the impact of the DMCA on academic encryption research. For the purpose of this Article, let us assume that the basic objective of the anti-circumvention provisions—the desire to help copyright owners use technology to protect their works—is a good one, or at least unobjectionable. In pursuing this objective, what impact does the DMCA, as currently drafted, have on the ability of academic encryption researchers to pursue

1. Digital Millennium Copyright Act, 17 U.S.C. §§ 101-1205 (2000).

2. *Id.* § 1201.

3. The DMCA contains several additional provisions, unrelated to the anti-circumvention provisions that are the subject of this Article. *See, e.g., Id.* § 512. For purposes of saving space, any mention of the DMCA in this Article references the anti-circumvention provisions.

4. *See, e.g.,* JESSICA LITMAN, *DIGITAL COPYRIGHT* (2001); Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813 (2001); *cf.* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519 (1999).

5. *See, e.g., WIPO Copyright Treaties Implementation Act: Hearings on H.R. 2281 Before the House Comm. on Commerce Subcomm. on Telecommunications, Trade and Consumer Prot. House Commerce Comm.*, 104th Cong. (1998) [hereinafter *Hearings on H.R. 2281*] (statements of Steven J. Metalitz representing the Motion Picture Association of America and Robert W. Holleyman, II of the Business Software Alliance), available at http://www.ipmall.info/hosted_resources/June5-98Hearing.pdf (last visited May 4, 2003); *cf.* David Nimmer, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 CARDOZO L. REV. 909, 927 (2002) (noting that "the DMCA enjoys widespread support from the motion picture, recording, software, and publishing industries").

their scientific research? And how should we evaluate this impact, as a normative matter?

Recently, there has been some debate over the extent to which academic encryption researchers should reasonably fear liability under the DMCA for certain forms of research. Although the DMCA contains an express exemption for encryption research,⁶ many encryption researchers have argued that the exemption is too narrow to be of practical use.⁷ Moreover, a number of recent cases have spurred fears among researchers that, despite the exemption, they may be liable for activities they routinely undertake in the course of their research.⁸ Other commentators, however, have argued that these fears are unwarranted under a proper reading of the statute, and that such fears may be exaggerated by DMCA critics to increase opposition to the DMCA.⁹

In this Article, I argue that, under certain circumstances, academic encryption researchers can continue to conduct and publish certain types of research without much practical risk of DMCA liability. This conclusion rests in part on a close reading of the statute and on predictions about how courts will likely interpret these statutory provisions in the context of academic encryption research. This conclusion also rests in part on an assessment of practical considerations surrounding DMCA litigation, such as the negative publicity such lawsuits tend to engender in light of recent, prominent cases. Thus, practically speaking, certain types of academic encryption research can still occur under the DMCA.

However, the DMCA *does* have a non-trivial impact on the conditions under which such research takes place. Specifically, the DMCA: imposes additional hurdles, which researchers must overcome before engaging in and publishing their research; limits the universe of individuals with whom researchers can freely communicate about their research; requires disclosure of the intention to engage in research and the fruits of such research to third-parties; affects the content of academic research papers; and limits avenues for publication of the research. Thus, even though academic encryption researchers can continue to conduct and publish some of their research under the DMCA without significant practical risk of criminal or civil liability, the DMCA significantly affects the manner in which that research is conducted.

6. See 17 U.S.C. § 1201(g).

7. See *infra* Part II.B.

8. See *infra* Part II.C.

9. See, e.g., Declan McCullagh, *Debunking DMCA Myths*, CNET NEWS.COM (Aug. 19, 2002), at <http://news.com.com/2010-12-950229.html> [hereinafter McCullagh, *Debunking DMCA Myths*].

Are these additional burdens on encryption research justified? In this Article, I will argue that they are not. I will argue that we should be extremely hesitant to impose any burdens on the conduct of basic scientific research in order to further an interest in the protection of intellectual property rights. Indeed, the DMCA represents a rather radical attempt by Congress to regulate not just copyright infringement or even the tools that facilitate infringement, but the basic research that could potentially be used to create tools that facilitate infringement. By imposing even minimal burdens on activity that is so far upstream from the actual infringing activity, we risk affecting many collateral areas of technology that are unrelated to the purported harm of copyright infringement.

From these conclusions, I argue that academic encryption researchers should have the widest possible freedom to conduct, discuss, and disseminate their research. Rather than placing any conditions on the research itself, the DMCA should focus on regulating concrete and problematic applications of the fruits of such scientific research. Any regulation of encryption research should be narrowly limited to distinguishing such research from activities that are clearly intended to facilitate infringement. The DMCA's encryption research exemption purports to do this, but in fact does much more. This recommendation could be implemented through proposed amendments to the DMCA or, alternatively, through expansive judicial interpretations of the encryption research exemption.

Although the topic of this Article is narrow, it is an important one. Encryption is a vital component of our current communications infrastructure.¹⁰ Anything that affects the ability of scientists to study and improve encryption technology therefore deserves careful scrutiny. More broadly, a close look at the DMCA's impact on encryption research can generate useful insights into the DMCA's overall regulatory approach. This Article focuses specifically on academic encryption researchers because nearly everyone agrees that the DMCA should leave their activities largely unaffected.¹¹ By studying whether the DMCA in fact successfully does so, this Article can shed some interesting light on how we should think about intellectual property protection and its collateral effects on scientific research.

10. See, e.g., Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution*, 143 U. PENN. L. REV. 709 (1995).

11. The distinction between “academic” and “nonacademic” encryption researchers is developed more fully *infra* in Parts III.B and IV.

II. BACKGROUND ON THE DMCA AND ENCRYPTION RESEARCH

A. The DMCA and the Encryption Research Exemption

In 1998, Congress passed the DMCA in response to perceived challenges presented by digital and network technologies.¹² The DMCA lends additional legal support to copyright owners' efforts to protect their works using technology. It does so by imposing liability on individuals who circumvent access control technologies, such as encryption.¹³ It also imposes liability for the dissemination of devices or technologies that are primarily designed for the purpose of, or have few commercially viable uses other than, facilitating such circumvention.¹⁴ Finally, the DMCA contains provisions that impose liability for removing or altering "copyright management information" attached to copyrighted files.¹⁵

When the bill that eventually became the DMCA was first introduced, it contained no exemption for encryption research. This was partly because Congress believed that the DMCA would rarely interfere with encryption research, since it thought that such research would not typically involve circumventing protection mechanisms actually deployed in commerce.¹⁶ However, members of the encryption research community testified at hearings, expressing concern that the DMCA would hinder their efforts, since much valuable research is performed on systems as they are actually deployed in the field.¹⁷ Indeed, this kind of real-world testing is the only way to find out whether an encryption system is secure.

12. I will begin here with a brief background on the DMCA and the encryption research exemption. Those already familiar with this material may wish to skip to the next section. I focus here primarily on the legal background. For general background on cryptography and encryption research, see Brief of Amici Curiae Dr. Steven Bellovin et al., Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (No. 00-9185) [hereinafter Cryptographers' Brief], available at <http://cyber.law.harvard.edu/openlaw/DVD/NY/appeals/010126-cryptographers-amicus.pdf> (last visited May 5, 2003) and BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY (2d ed. 1996).

13. 17 U.S.C. § 1201(a)(1) (2000).

14. *See id.* §§ 1201(a)(2), 1201(b).

15. *Id.* § 1202.

16. *See S. REP. NO. 105-190, 1998 WL 239623, at *15-16 (1998).*

17. *See, e.g., Hearings on H.R. 2281, supra note 5, at 4-6.* Jonathan Callas testified: In order to ensure that a cryptographic system has no weaknesses, either in the cryptography itself or in its application and implementation, it is essential that we continually attempt to break that system.

....

As a result of this testimony, the final version of the DMCA contained an express exemption for encryption research.¹⁸ The exemption shields encryption researchers from liability for circumventing access-control technologies under certain circumstances.¹⁹ The exemption defines “en-

It is essential to test technology as it is applied—i.e. when it is being used to protect something, because most weaknesses in cryptography occur in its application.

Id. (emphasis original), available at http://www.ipmall.info/hosted_resources/June5-98Hearing.pdf (last visited May 4, 2003); see also Cryptographers’ Brief, *supra* note 12, at 29-30, available at <http://cyber.law.harvard.edu/openlaw/DVD/NY/appeals/010126-cryptographers-amicus.pdf> (“The advancement of the science of cryptography depends on researchers’ ability to study signals ‘in the wild,’ not only those codes developed for academic purposes, since the implementation may be as important as the algorithm in determining a system’s security.”).

18. It is worth noting that the European Union Directive and certain implementations of the WIPO treaties regarding anti-circumvention legislation contain no exemption for encryption research.

19. 17 U.S.C. § 1201(g) states:

Encryption research.

(1) Definitions. For purposes of this subsection—

(A) 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

(B) the term “encryption technology” means the scrambling and de-scrambling of information using mathematical formulas or algorithms.

(2) Permissible acts of encryption research. 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 . . . of a published work in the course of an act of good faith encryption research if—

(A) the person lawfully obtained the encrypted copy . . . ;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section

(3) Factors in determining exemption. In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(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

“encryption research” as “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.”²⁰ Encryption research is exempt from liability for circumvention if it is conducted in “good faith,” provided that the encrypted copy is lawfully obtained, the act of circumvention is “necessary” for the research, and the researcher made a good faith effort to obtain authorization from the copyright owner before engaging in the circumvention.²¹

In determining whether the exemption applies, Congress directed courts to consider a number of factors,²² including the manner in which information derived from the research is disseminated and whether the researcher “is engaged in a legitimate course of study, employed, or is appropriately trained or experienced, in the field of encryption technol-

(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; and

(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.

(4) Use of technological means for research activities. Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to—

(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and

(B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).

Id.

20. *Id.* § 1201(g)(1)(A).

21. *Id.* § 1201(g)(2)(A)-(C).

22. The precise role played by the factors in § 1201(g)(3) is not entirely clear from the text of the statute. The specific requirements for the exemption are listed in § 1201(g)(2), and one would expect that satisfaction of these requirements would be sufficient for the exemption to apply. However, § 1201(g)(3) goes on to list additional “factors,” which a court should consider in determining whether an individual “qualifies for” the exemption. This suggests that these additional factors play some role, although it is not clear precisely what role, since § 1201(g)(2) appears self-contained and does not seem to contemplate consideration of these additional factors. One way of perhaps understanding these additional factors is as a gloss on the general “good faith” requirement in § 1201(g)(2).

ogy.”²³ The DMCA further permits researchers to develop the tools necessary to engage in such research and to share such tools with “another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research.”²⁴ This last provision shields the researcher from liability under the “tools” provision of the DMCA.²⁵ Finally, the exemption directs the Register of Copyrights to study the impact of the DMCA on encryption research and to report back to Congress within one year of enactment.²⁶

The exemption was essentially an attempt by Congress to preserve some freedom for encryption research while ensuring that the exemption would not create a loophole for illegitimate attempts to exploit vulnerabilities under the cover of encryption research.²⁷ The House Commerce Report recognized that the DMCA, as originally drafted, had the potential to stifle encryption research and thereby cause substantial harm. Moreover, after hearing testimony by encryption researchers, the House Commerce Committee believed that encryption researchers needed the ability to test encryption technologies not just under laboratory conditions, but also as they are applied in the real world.²⁸ The exemption was thus an attempt to

23. 17 U.S.C. § 1201(g)(3)(A)-(C).

24. *Id.* § 1201(g)(4)(A)-(B).

25. *Id.* § 1201(a)(2).

26. *See id.* § 1201(g)(5).

27. *See H.R. REP. NO. 105-511 (II), 1998 WL 414916, at *26-27, *43-44 (1998) [hereinafter House Commerce Report 511].*

28. *Id.* at *27. The Report states:

The effectiveness of technological protection measures to prevent theft of works depends, in large part, on the rapid and dynamic development of better technologies, including encryption-based technological protection measures. The development of encryption sciences requires, in part, ongoing research and testing activities by scientists of existing encryption methods, in order to build on those advances, thus promoting and advancing encryption technology generally. This testing could involve attempts to circumvent or defeat encryption systems for the purpose of detecting flaws and learning how to develop more impregnable systems. The goals of this legislation would be poorly served if these provisions had the undesirable and unintended consequence of chilling legitimate research activities in the area of encryption.

In many cases, flaws in cryptography occur when an encryption system is actually applied. Research of such programs as applied is important both for the advancement of the field of encryption and for consumer protection. Electronic commerce will flourish only if legitimate encryption researchers discover, and correct, the flaws in encryption systems before illegitimate hackers discover and exploit these flaws. Accord-

strike a balance and to sort out “legitimate” encryption research from “illegitimate” hacking that would lead to increased piracy.²⁹

B. Criticism of the DMCA and the Exemption

Since passage of the DMCA, many legal and scientific commentators have criticized the exemption for being both too narrow and too vague, thereby chilling legitimate scientific encryption research.³⁰ Commentators have critiqued the exemption on several grounds.³¹ First, many commenta-

ingly, the Committee has fashioned an affirmative defense to permit legitimate encryption research.

Id.

29. *Id.* at *44. The Report states:

The Committee recognizes that courts may be unfamiliar with encryption research and technology, and may have difficulty distinguishing between a legitimate encryption researcher and a so-called ‘hacker’ who seeks to cloak his activities with this defense. Section 102(g)(3) therefore contains non-exclusive list of factors a court shall consider in determining whether a person properly qualifies for the encryption research defense.

Id.

30. See, e.g., Cryptographers’ Brief, *supra* note 12 at 9-10, 27-29, available at <http://cyber.law.harvard.edu/openlaw/DVD/NY/appeals/010126-cryptographers-amicus.pdf>; COMM. ON INTELL. PROP. RIGHTS & EMERGING INFO. INFRASTRUCTURE, NAT’L RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE 2 (Nat’l Academy Press, available at <http://books.nap.edu/books/0309064996/html/2.html/index.html>, 2000); Cassandra Imfeld, *Playing Fair With Fair Use? The Digital Millennium Copyright Act’s Impact on Encryption Researchers and Academicians*, 8 COMM. L. & POL’Y 111 (2003); Michael Landau, *Has the Digital Millennium Copyright Act Really Created a New Exclusive Right of Access?: Attempting to Reach a Balance Between Users’ and Content Providers’ Rights*, 49 J. COPYRIGHT SOC’Y U.S.A. 277, 306-09 (2001); Pamela Samuelson, *Anti-Circumvention Rules: Threat to Science*, 293 SCI. 2028 (2001); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519 (1999); Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1647-49 (2002); Brian Bolinger, Comment, *Focusing on Infringement: Why Limitations on Decryption Technology Are Not the Solution to Policing Copyright*, 52 CASE W. RES. L. REV. 1091 (2002); Michael Landau, *The DMCA’s Chilling Effect on Encryption Research*, at <http://www.gigalaw.com/articles/2001-all/landau-2001-09-all.html> (last visited May 5, 2003).

31. Many of these objections were expressed in the comments to the Register of Copyrights, which were solicited in fulfillment of the Copyright Office’s statutory duty to report, within one year of the DMCA’s enactment, on the impact of the DMCA on encryption research. See NAT’L TELECOMM. INFO ADMIN. & U.S. COPYRIGHT OFFICE, REPORT TO CONGRESS: JOINT STUDY OF SECTION 1201(G) OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, at <http://www.copyright.gov/reports/studies>; Comments of Jonathan D. Callas, at <http://www.copyright.gov/reports/studies/comments/012.pdf> (July 26, 1999) [hereinafter Callas Comment]; Comments of EMusic.com, Inc., at <http://www.copyright-.>

tors have argued that the definitions of encryption and encryption research are too narrow. In particular, they have taken issue with the requirement that the act of circumvention be “necessary” for the research. The fear is that researchers will be chilled if they feel the need to prove that the act was “necessary,” as opposed to being merely important or useful.³²

Second, commentators have criticized the requirement that a researcher first seek authorization from the copyright owner before engaging in the act of circumvention. They question whether this amounts to a requirement that the copyright owner approve of the circumvention, in which case the exemption will be meaningless.³³ On the other hand, if, as the text of the exemption suggests, all that is required is a request and not approval, then the requirement serves no purpose other than to place the copyright owner on notice, thereby inviting a potential lawsuit or the imposition of burdensome conditions and limitations on dissemination of the research.³⁴ In either case, the requirement is problematic as it may chill legitimate research.

gov/reports/studies/comments/010.pdf (July 26, 1999) [hereinafter EMusic.com Comment]; Comments of the Computer & Communications Indus. Ass’n (CCIA) at <http://www.copyright.gov/reports/studies/comments/011.pdf> (submitted July 26 1999) [hereinafter CCIA Comment]; Comments of Hal Finney, at <http://www.copyright.gov/reports/studies/comments/003.pdf> (July 12, 1999) (“Prudent researchers who do not want to risk criminal prosecution will avoid work in this area The result will be a loss of confidence in cryptographic technology as users realize that the best and brightest researchers are no longer able to do research in this field. This will harm electronic commerce and damage American interests domestically and internationally.”) [hereinafter Finney Comment]; Comments of Kroll O’Gara Information Security Group, at <http://www.copyright.gov/reports/studies/comments/007.pdf> (submitted July 26, 1999) [hereinafter O’Gara Comment]; Comments of David Wagner, at <http://www.copyright.gov/reports/studies/comments/001.pdf> (May 27, 1999) (“As an encryption researcher, I don’t think I will be going out on a limb to predict that this law is about to have a negative effect on encryption research”) [hereinafter Wagner Comment]. However, the Register ultimately concluded that these concerns were still hypothetical, they had already been raised when the DMCA was being considered, and there was as yet no concrete evidence, nor were there specific examples, of encryption research being hindered in any way. As the Register recognized, this was not surprising, given that the report was due one year before the anti-circumvention provisions were to go into effect.

32. See Finney Comment, *supra* note 31.

33. *Id.* (“Provision (C) can only be described as bizarre. There is no requirement elsewhere in the exemptions to receive authorization from the copyright holder. Apparently, whether authorization is granted or not makes no difference, but nevertheless the researcher is required to seek authorization? This is completely illogical.”); see also Cal-las Comment, *supra* note 31.

34. Bolinger, *supra* note 30, at 1097-98 (“Although sharing one’s results with the party most affected by them is reasonable given the general policy goal of improving and

Third, commentators have taken issue with the additional factors—particularly the factor that looks to the training or affiliation of the researcher—used to determine whether a researcher “qualifies” under the exemption. This is because encryption research is characterized, somewhat unusually, by the active participation of individuals or “hobbyists” who are not affiliated with a research organization or who may not have had any formal training. Indeed, such individuals commonly play a significant role in testing the security of implemented systems and publicizing weaknesses in such systems.³⁵

Fourth, commentators argued that the exemption is ambiguous regarding the extent to which researchers may publish or share their results with others. The exemption itself hints that dissemination of information may be permissible so long as it is done in a manner that is “reasonably calculated to advance the state of knowledge or development of encryption technology.”³⁶ However, the exemption does not state this outright. Moreover, many commentators have argued that the exemption from liability under the tools provision is too narrow.³⁷ According to these commentators, an essential part of publishing the results of encryption research is providing others with the tools to verify and comment upon the results. Frequently this involves sharing either actual code or descriptions that are sufficiently detailed to enable others to create their own code.³⁸ These activities could lead to liability under the tools provision. Furthermore, the

strengthening encryption techniques, under the present state of the law, such an action is tantamount to an invitation to be sued.”).

35. See Cryptographers’ Brief, *supra* note 12, at 24, available at <http://cyber.law.harvard.edu/openlaw/DVD/NY/appeals/010126-cryptographers-amicus.pdf> (“The exception of 1201(g) endorses a fundamentally mistaken conception of cryptographic science, one in which advances are predictable, generated only from within an ‘establishment,’ and where limited, strictly regulated testing suffices to assure the security of cryptosystems.”); Callas Comment, *supra* note 31 (“An interesting aspect of today’s research is that relative unknowns do some of the most important new work.”).

36. 17 U.S.C. § 1201(g)(3)(A) (2000).

37. See, e.g., Cryptographers’ Brief, *supra* note 12, at 14, available at <http://cyber.law.harvard.edu/openlaw/DVD/NY/appeals/010126-cryptographers-amicus.pdf>. The Brief states:

The science of cryptography depends on cryptographers’ ability to exchange ideas in code, to test and refine those ideas, and to challenge them with their own code. By communicating with other researchers and testing each others’ work, cryptographers can improve the technologies they work with, discard those that fail, and gain confidence in technologies that have withstood repeated testing.

Id.

38. *Id.*

exemption is too narrow insofar as it limits such sharing only to collaborators and not to the wider research community.

Fifth, commentators have expressed concern that the exemption is incomplete as it only applies to liability under § 1201(a) for circumventing access-control technologies, but does not apply to liability under § 1201(b) for distribution of devices that circumvent copy-control technologies.³⁹ Some forms of research might well give rise to liability under both provisions.⁴⁰ Nor does the exemption apply to liability under § 1202, which involves the integrity of copyright management information.⁴¹ For example, the provision would not shield from liability a researcher who wished to remove a digital watermark containing copyright management information. Thus, an encryption researcher may be shielded from liability under § 1201(a), but still subject to liability under these alternative provisions.

Finally, commentators have argued that the above flaws would have a chilling effect on encryption research without any offsetting benefit in the form of added security for copyright owners. The testing of implemented systems can still take place in other countries, since the DMCA's impact is largely limited to the United States, and many other countries have no equivalent statute. Moreover, individuals will continue to attack and exploit the weaknesses of such systems anonymously. Given the ease with which one can distribute information about the weaknesses of encryption systems over the Internet, the DMCA will do little to reduce the incidence of circumvention or the availability of circumvention technologies.

Indeed, according to commentators, the DMCA will actually make encryption technologies more susceptible to such attacks, since copyright owners will not be able to improve their systems using the results of open and legitimate encryption research. That is, by chilling legitimate encryption research, the DMCA will simply drive encryption research into less legitimate channels. Weaknesses discovered by attackers will not be published and reviewed in academic journals or on the Internet. Consequently, individuals and companies will never be confident that any proposed or implemented systems are robust and secure.⁴²

39. See generally Bolinger, *supra* note 30, at 1100.

40. See R. Anthony Reese, *Legal Incentives for Adopting Digital Rights Management Systems: Merging Access Controls and Rights Controls*, 18 BERKELEY TECH. L.J. 619, 622-27 (2003) (analyzing in detail the ways in which implemented systems may be protected as both access and rights control technologies).

41. 17 U.S.C. § 1202(b).

42. See EMusic.com Comment, *supra* note 31. EMusic.com states:

While there is a superficial appeal to the argument that these security implementations would have had a longer shelf-life had their vulnerabilities *not* been revealed, in the long run, there is greater benefit from

C. Initial Cases Implicating the Exemption

Despite these objections, the anti-circumvention provisions of the DMCA went into effect in October of 2000, and since then a few cases implicating the encryption research exemption have arisen. The first case to consider the encryption research exemption did so only briefly. That case, *Universal City Studios, Inc. v. Reimerdes*,⁴³ involved a DMCA claim against the publication and distribution of DeCSS, a program that enabled decryption of DVDs. DeCSS was created by a Norwegian programmer, ostensibly to permit individuals to play DVDs on the Linux operating system, and then posted on a website by the defendants. One of the defendants' arguments was that DeCSS represented legitimate encryption research.⁴⁴ The court quickly rejected this argument, emphasizing the defendants' failure either to seek permission from or to provide the results of their research to the copyright owners.⁴⁵

The second case involving the exemption occurred in a context better suited to the exemption. *Felten v. RIAA*⁴⁶ concerned the activities of a number of academic encryption researchers who cracked a watermarking technology called SDMI, which the recording industry was planning to deploy in order to protect recorded music from being copied. The recording industry had issued a public challenge inviting individuals to try to crack the technology. The plaintiffs were a team of researchers from various institutions, including Princeton and Rice, who took up that challenge and succeeded. When they tried to publish an academic paper detailing their research, they received a threatening letter from the RIAA, which claimed that publication of the paper could result in liability under the DMCA. In response, the researchers withdrew their paper from an academic conference. They later filed suit against the RIAA, seeking a decla-

having those vulnerabilities revealed. This is particularly true when reliance on a particular security implementation could lead to significant industry and consumer investment in hardware and software devices that support that implementation.

Id. at 4 (emphasis original); see Finney Comment, *supra* note 31 ("By driving the legitimate experts into other avenues of research, the DMCA will leave the field to those who care nothing about laws. To paraphrase another slogan, if you outlaw cryptographic research, only outlaws will do cryptographic research.").

43. 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

44. *See id.* at 320-21.

45. *See id.* at 321.

46. Compl. Declaratory J. and Injunctive Relief, *Felten* (No. CV-01-2669), available at http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html.

ration that their activities did not violate the DMCA. After much back-and-forth, the RIAA eventually acceded to the publication of the paper, and the case was dismissed.⁴⁷

The third case was a criminal prosecution against Dmitri Sklyarov, a Russian programmer.⁴⁸ Sklyarov had cracked the technological protection measure used by Adobe to control access to copyrighted content distributed in its eBook format. The Russian company he worked for distributed his circumvention software over the Internet. When Sklyarov traveled to the United States to present a paper on his research at a conference, he was arrested and charged with criminal violations of the DMCA. Although Sklyarov eventually reached an agreement with the U.S. government, prosecution continued against Sklyarov's company, Elcomsoft. After trial, the jury acquitted Elcomsoft based on a finding that the corporation did not satisfy the statutory intent requirement for criminal liability.⁴⁹

In addition to the cases above, a number of other incidents implicating the DMCA and encryption research have been reported in the press.⁵⁰

Although all of the cases above implicate, to some extent, the encryption research exemption, none resulted in an opinion comprehensively interpreting the exemption in the context of academic encryption research. Accordingly, uncertainty persists regarding the precise extent to which encryption research is privileged under the DMCA.

D. Responses by Encryption Researchers

The cases above, along with the criticisms of the encryption research exemption, have led to a good deal of concern within the encryption research community. In particular, a number of encryption researchers have refused to publish their research results in response to concerns about

47. For additional information about *Felten*, including the court filings, court orders, and other resources, see the Electronic Frontier Foundation's website at http://www.eff.org/IP/DMCA/Felten_v_RIAA/ (last visited Apr. 27, 2003).

48. Compl., United States v. Elcomsoft, 203 F. Supp. 2d 1111 (N.D. Cal. 2002) (No. 5-01-257), available at http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20010707_complaint.html (last visited May 5, 2003).

49. For additional information about *Sklyarov*, see the Electronic Frontier Foundation's website at http://www.eff.org/IP/DMCA/US_v_Elcomsoft/ (last visited Apr. 27, 2003).

50. See, e.g., Declan McCullagh, *HP Backs Down on Copyright Warning*, CNET NEWS.COM (Aug. 1, 2002), at <http://news.com.com/2100-10230947745.html> (describing how Hewlett-Packard backed off from initial DMCA threat against researchers for publishing information on flaw in operating system) [hereinafter McCullagh, *HP Backs Down*]; cf. David Becker, *MIT Student Hacks into Xbox*, CNET NEWS.COM (June 3, 2002), at <http://news.com.com/2100-1040-931296.html> (describing MIT student publication of paper on security flaws in the Microsoft Xbox).

DMCA liability.⁵¹ For example, the Dutch cryptographer Niels Ferguson declined to publish the results of research he had conducted regarding High Bandwidth Digital Content Protection, a system used by Intel to encrypt video. Ferguson, an independent cryptography consultant, indicated that he had found weaknesses in that system, but decided not to publish the results and removed all references to this research from his website for fear of DMCA liability.⁵² Other researchers have similarly indicated that they have withheld or declined to publish their research results out of the same concern.⁵³

Professional associations and conferences have also modified their practices in response to the fear of DMCA liability. Some encryption researchers have suggested boycotting encryption research conferences held in the United States.⁵⁴ Some conference organizers have decided to hold their conferences outside the U.S., in order to minimize concerns about liability. In addition, in November 2001, the Institute of Electrical and Electronics Engineers (IEEE), a major publisher of computer science journals, began requiring that all authors indemnify the IEEE for DMCA liability resulting from the publication of their research in the journal. The IEEE later withdrew this requirement in response to widespread objections.⁵⁵

51. See generally Elec. Frontier Found., *Unintended Consequences: Four Years Under the DMCA*, at http://www.eff.org/IP/DMCA/20030103_dmca_consequences.pdf (last visited May 4, 2003) [hereinafter Elec. Frontier Found., *Unintended Consequences*].

52. See Niels Ferguson, *Censorship in Action: Why I Don't Publish My HDCP Results* ("I have written a paper detailing security weaknesses in the HDCP content protection system. I have decided to censor myself and not publish this paper for fear of prosecution and/or liability under the US DMCA law."), at <http://www.macfergus.com/nieles/dmca> (Aug. 15, 2001); see also Lisa Bowman, *Researchers Weigh Publication, Prosecution*, CNET NEWS.COM (Aug. 15, 2001), at <http://news.com.com/2100-1023-271712.html>.

53. See Robert Lemos, *Security Workers: Copyright Law Stifles*, CNET NEWS.COM (Sept. 6 2001), at <http://news.cnet.com/2100-1001-272716.html>; Wade Roush, *Breaking Microsoft's e-Book Code*, TECH. REV. (Nov. 1, 2001), at 24, available at <http://www.technologyreview.com/articles/innovation11101.asp>. See generally Elec. Frontier Found., *Unintended Consequences*, *supra* note 51, at 3-4 (describing how Fred Cohen, a well-respected professor of digital forensics and consultant, and Dug Song, a network security protection expert, removed content from their websites fearing liability).

54. See Will Knight, *Computer Scientists Boycott U.S. Over Digital Copyright Law*, NEW SCIENTIST (July 23, 2001), available at <http://www.newscientist.com/news/news.jsp?id=ns99991063>; see also Elec. Frontier Found., *Unintended Consequences*, *supra* note 51, at 4 (discussing encryption researcher reaction to the arrest of Sklyarov).

55. Will Knight, *Controversial Copyright Clause Abandoned*, NEW SCIENTIST (Apr. 15, 2002), available at <http://www.newscientist.com/news/news.jsp?id=ns99992169>; see also Elec. Frontier Found., *Unintended Consequences*, *supra* note 51, at 4.

The above responses indicate that many encryption researchers are in fact worried about potential liability. Indeed, some have indicated that they are avoiding research topics that might implicate DMCA liability. As encryption researcher David Wagner put it in his comments submitted to the Register of Copyrights:

As an academic researcher, I personally find it a little scary to consider doing research on copyright protection schemes, because of 1201(g). I analyze real-world security systems. If, in doing so, I discover a weakness in some deployed system, I face an unsavory choice: tell no one, or publish. If I decide to publish, I have to worry about the threat of retaliation from those trying to sell the flawed system. Whether or not I would eventually win in court, the threat of having to spend time and money on a lawsuit is enough to make me tend to shy away from studying copyright protection.⁵⁶

Despite these claims about the chilling effect of the DMCA on encryption researchers, a number of commentators have recently suggested that such fears of liability are greatly exaggerated and that there is no real risk to academic encryption researchers for the conduct and publication of their research.⁵⁷ Pointing to the text of the DMCA, these commentators argue that it would be a significant stretch for a court to find the mere publication of a research paper a violation of the “tools” provision of the DMCA. Moreover, the risk of criminal liability under the DMCA appears to be extremely low, if not non-existent, given past enforcement patterns and government statements regarding criminal liability for research.⁵⁸ According to these commentators, encryption researchers should feel comfortable publishing their results.⁵⁹ Some commentators have even suggested that DMCA critics have intentionally exaggerated its potential scope in order to increase opposition to the law.⁶⁰

56. Wagner Comments, *supra* note 31.

57. See McCullagh, *Debunking DMCA Myths*, *supra* note 9, at <http://news.com.com/2010-12-950229.html>.

58. *See id.* (“The risk that a researcher could go to jail for giving a speech at an academic conference is essentially zero.”) (quoting George Washington University law professor Orin Kerr).

59. *See id.*

60. *See id.* (quoting Allan Adler of the Association of American Publishers as stating that “[EFF] succeeded in creating a kind of chilling effect in the scientific community because of the kind of fear-mongering they were engaged in.”).

III. IMPACT OF THE DMCA ON ENCRYPTION RESEARCH

Are the fears of academic encryption researchers reasonable or exaggerated? More broadly, what impact can we reasonably expect the DMCA to have on academic encryption research? In this part of the Article, I argue that, under certain circumstances, academic encryption researchers can continue to conduct and publish certain types of research without significant fear of legal liability or much practical risk of being sued. At the same time, however, the DMCA has a significant impact on the conditions under which such research is conducted. Although the DMCA does not *prevent* academic encryption research, it does *regulate* it—and it is this more subtle impact of the DMCA that we should be concerned about.

A. Academic Encryption Research Can Still Take Place

In assessing whether encryption researchers face a realistic risk of DMCA liability, the first step is to determine the substantive basis for these concerns. That is, based on a close reading of the statute, legislative history, and limited case law, how likely is it that a court would find an academic encryption researcher liable under the DMCA for conducting and publishing his or her research?⁶¹ To answer this question, it may be useful to look at three separate acts of the researcher, each of which may give rise to potential DMCA liability: the act of circumvention; the creation of a tool used to circumvent; and the publication of the results.

With respect to the act of circumventing the access control technology (otherwise prohibited under § 1201(a)(1)), an encryption researcher should be able to circumvent the access control technology without much fear of liability if the researcher abides by the requirements spelled out in the encryption research exemption. In particular: the researcher must lawfully obtain the encrypted copy of the material he wishes to analyze; the act of circumvention must be necessary to the conduct of such research; the researcher must make a good faith attempt to obtain authorization before circumvention; and the act of circumvention must not otherwise constitute

61. Note that I focus narrowly on academic encryption researchers because much of the recent debate has focused on the impact of the DMCA on this group of researchers. This is not surprising, since nearly all sides of the debate appear to acknowledge that, whatever the impact of the DMCA might be on other encryption researchers, any impact on this core set of researchers would be very problematic—the only difference of opinion is over the scope and extent of that impact. Accordingly, I do not address the (in my view, quite legitimate) concerns that other, nonacademic encryption researchers will find it even more difficult to engage in research, except to the extent that this limitation affects academic researchers. I do not address this latter question because I eventually conclude that the DMCA in fact does affect the behavior of the core set of academic encryption researchers and that this, in itself, is extremely problematic.

copyright infringement or the violation of other applicable law.⁶² In addition, the researcher should seek to satisfy the factors that a court is directed to consider in determining whether the exemption applies: the manner in which information about the research was disseminated; whether the researcher has appropriate training and experience in the field; and whether and when the researcher provided notice of the results of the research to the copyright owner.⁶³

Together, these requirements raise a number of hurdles, but an academic encryption researcher should in most cases be able to overcome them. Obtaining a lawful copy will rarely be a problem for copies that are widely available to consumers.⁶⁴ A good faith attempt to obtain authorization would entail sending notice to the copyright owner, but probably not much more than that, as nothing in the statute suggests that the copyright owner must give such authorization (indeed, such a reading would be plainly inconsistent with the exemption). The provision regarding violation of other laws essentially poses no additional restriction, since a researcher violating such laws would already be separately liable.

Of these requirements, the “necessity” requirement is perhaps the most problematic. Researchers have voiced fear that they will be required to prove their actions are in fact “necessary” rather than simply “useful” or “helpful.” This is a valid concern. However, in many cases researchers can meet the necessity requirement as, for example, when a researcher is testing the security of encryption as implemented on a protected copy. Almost by definition, it will be *necessary* in such a case to circumvent the protection mechanism in order to test its security. Moreover, one can reasonably expect the courts to give some deference to scientific judgments regarding what is or is not necessary in the conduct of scientific research.

The additional factors in the exemption also generally weigh in favor of academic encryption researchers. Publication of the work in an academic journal would satisfy the factor that looks to the manner of dissemination. Training in the field would be satisfied, certainly, in the case of an

62. See 17 U.S.C. § 1201(g)(2)(A)-(D) (2000).

63. See *id.* § 1201(g)(3)(A)-(C). I am assuming here that the researcher’s activities fall within the definition of “encryption research” in accordance with § 1201(g)(1). A number of commentators have argued that the definition in the statute is too narrow. I address this issue in more detail below.

64. Note that this may arguably not be the case if a copy is obtained in violation of a shrinkwrap or other license. Moreover, this raises the broader question regarding the enforceability of shrinkwrap terms that prohibit reverse engineering or research. See, e.g., *Bowers v. Baystate Techs., Inc.*, 302 F.3d 1334, 1341 (Fed. Cir. 2002) (holding that the Copyright Act does not preempt a contractual prohibition on reverse engineering). These questions are beyond the scope of this Article.

academic encryption researcher.⁶⁵ Finally, the researcher could easily meet the third and final requirement by sending the copyright owner a copy of the research paper or otherwise notifying it of the research results. Thus, the exemption provides a fairly clear roadmap for an encryption researcher who wishes to ensure that he or she will face no liability for the act of circumvention.

Similarly, an encryption researcher should be able to create the tools necessary to engage in the act of circumvention. For example, say that a researcher, in order to crack an encrypted file, has to create a program to enable such cracking. The creation of such a program could well violate § 1201(a)(2), since it could constitute “manufactur[ing] . . . any technology . . . that . . . is primarily designed . . . for the purpose of” circumvention.⁶⁶ However, § 1201(g)(4) gives the researcher the right to “develop and deploy” circumvention technology “for the sole purpose of . . . performing the acts of good faith encryption research,” thereby exempting the creation of the cracking program from liability. Moreover, the exemption permits the researcher to give the program to another person “with whom he or she is working collaboratively” for purposes of research or verification.⁶⁷

Finally, publication of the research should be possible under the DMCA as well. The question would be whether publishing an academic paper would give rise to liability under the “tools” provision of the DMCA—i.e., would an academic paper describing weaknesses in an encryption technology constitute an “offer to the public” of “any technology . . . that . . . is primarily designed . . . for the purpose of circumventing” or “has only limited commercially significant purpose . . . other than to circumvent.”⁶⁸ The argument in support of liability would be that the paper’s description of the decryption technique is a “technology” and that it is either primarily designed to circumvent or has limited commercially significant use other than to circumvent.

While it is not impossible that a court would adopt such an interpretation, it is highly unlikely. First, the legislative history indicates that when

65. It might not be satisfied in cases where a researcher is not so clearly affiliated with an academic or other research institution. As a number of critics have pointed out, this may be quite problematic in the field of encryption research, since many discoveries are made by individuals who do not have much in the way of formal training. For present purposes, I am focusing narrowly on the question of academic encryption researchers. I will address these other concerns later in this Article.

66. § 1201(a)(2). *But see* Reese, *supra* note 40 (suggesting that the creation of a single tool might not constitute a “manufacture”).

67. *Id.* § 1201(g)(4)(B).

68. *Id.* § 1201(a)(2)(A)-(B).

Congress enacted the “tools” provision, it very clearly had in mind so-called “black boxes” or other devices designed to permit consumers to engage in widespread circumvention.⁶⁹ In light of this legislative history, a court would be hard-pressed to read the provision to encompass a research paper. Second, there is a strong argument that a research paper is not “primarily designed . . . for the purpose of circumvention,” even if it describes the circumvention process. Instead, the primary purpose of the paper is to advance scientific research in the field of encryption.⁷⁰ Third, such an interpretation would be in considerable tension with the terms of the encryption research exemption, which strongly suggests that the publication of research results is permissible.⁷¹ For all of these reasons, it is highly unlikely that a court would impose liability under the DMCA for the publication of an academic paper.⁷²

Further, the legislative history behind the exemption provides strong general support for exempting academic research activities and publication. It clearly evinces a concern that the DMCA should not unduly hinder encryption research, and contains many statements along these lines.⁷³ Any application of the DMCA to hinder legitimate research or its publication would conflict expressly with the legislative history. Thus, looking at

69. House Commerce Report 511, *supra* note 27, at *38 (“The Committee believes it is very important to emphasize that Section 1201(a)(2) is aimed fundamentally at outlawing so-called ‘black boxes’ that are expressly intended to facilitate circumvention of technological protection measures for purposes of gaining access to a work.”).

70. This was the position adopted by the Department of Justice in its brief supporting dismissal of the *Felten* case:

Plaintiffs’ alleged conduct is not proscribed by the statute. [T]he DMCA prohibits trafficking in certain technologies that are primarily designed to circumvent copyright material access controls. By contrast, the Plaintiffs’ alleged objective is to strengthen, not circumvent, these access controls. While Plaintiffs’ computer programs have the additional capability of actually circumventing access controls, they are allegedly not designed or marketed for the purposes of actually getting access to the copyrighted material itself. They are designed and published to further scientific research into access controls. As a result, Plaintiffs’ alleged conduct is not proscribed by the DMCA.

Dep’t. of Justice Reply Br., *Felten v. Recording Indus. Assn. (RIAA)*, (D.N.J. filed June 6, 2001) (No. CV-01-2669), available at http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011108_doj_reply_brief.html (last visited May 5, 2003) (internal citations omitted).

71. See § 1201(g)(3)(A) (directing courts to consider “whether the information . . . 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”).

72. The separate issue of distribution of code is dealt with below.

73. See *supra* Part II.A.

both the text and the legislative history, it is unlikely that a court would read the DMCA to cover the research activities described above.

Finally, in predicting how courts would rule on a given legal issue, one should always be aware of the factual context and, in particular, how a court would likely view the parties before it. On this score, there is every reason to expect that courts would be favorably disposed to academic encryption researchers. In particular, academic encryption researchers do not look like the “hackers” that the statute is designed to target. Although one may question the validity of this distinction as a substantive matter, it is likely that such a distinction would have an impact on a court interpreting the scope of the DMCA. Indeed, the existing DMCA litigation suggests that courts are sensitive to the identities of the alleged infringers.⁷⁴ Ultimately, the probability of a court imposing DMCA liability upon an academic encryption researcher is quite low.

Of course, a low probability of liability does not necessarily mean that copyright owners will not bring or threaten to bring claims against researchers, even if such claims are weak. As a number of DMCA critics have pointed out, eventual success in court is not required to have a devastating effect on research.⁷⁵ All that is required is the filing or even the threat of a lawsuit. As we have already seen, copyright owners have indeed made threats against academic encryption researchers.⁷⁶ Even if the substantive basis for a suit is weak, its mere filing will force a researcher to expend significant resources in response. Moreover, since no court has yet definitively interpreted the precise scope of the encryption research exemption, ambiguities in the DMCA work to the advantage of the better-funded copyright owners.

While it is true that nothing prevents copyright owners or the government from bringing weak claims, there are good reasons to believe that the

74. Compare, for example, the very different treatment of the “hackers” in *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 321 (S.D.N.Y. 2000), *aff’d sub nom.* *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001) (“Neither of the defendants remaining in this case was or is involved in good faith encryption research . . . [a]ccordingly, defendants are not protected by section 1201(g.”)), and the scientists in *Felten*. See Elec. Frontier Found., *Summary of Felten v. RIAA*, at http://www.eff.org/IP/DMCA/Felten_v_RIAA (last visited Mar. 14, 2003) (“EFF is asking the court to affirm the right of these scientists to publicly present what they have learned.”). Of course, there are many other grounds for distinguishing these two cases.

75. See, e.g., Wagner Comments, *supra* note 31 (“[The] threat of having to spend the time and money on a lawsuit is enough to make [encryption researchers] shy away from studying copyright protection.”).

76. One example is the SDMI threat against Felten’s research group. See Elec. Frontier Found., *Unintended Consequences*, *supra* note 51, at 2.

risks of such claims or threats are rather low. First, the risk of criminal prosecution is, in reality, quite low. Although the government initiated a criminal prosecution against Dmitri Sklyarov, the facts of that case differ from the case of an academic encryption researcher. In that case, Sklyarov worked for a for-profit company that distributed a circumvention program to consumers. For criminal liability under the DMCA to attach, the government must prove an additional element of commercial gain, which is missing in most academic encryption researcher cases. Moreover, in intellectual property cases, the United States government usually confines its criminal prosecutions to the most egregious cases of large-scale infringement, where there is clearly a profit motive. Thus, it is hard to see much realistic risk of criminal liability.

Threat of civil liability may be more of a concern, but even there, the risk of threat is reduced by a number of factors. First, the weakness of the substantive case would certainly be a factor. Second, recent cases suggest that copyright owners are sensitive to the unfavorable publicity that often follows threats to scientific research. In a number of recent cases, private parties quickly withdrew threats of DMCA suits in the wake of significant public criticism. For example, in the *Felten* litigation, public outcry over the threat of DMCA liability quickly led the RIAA to back off from its initial threat. Similarly, Hewlett-Packard recently retracted its threat of DMCA liability against a group of individuals who had discovered a security flaw in one of its products, again in response to public objections.⁷⁷ And in the Sklyarov case, although Adobe initiated the criminal investigation by complaining to the government, it quickly withdrew its support for the prosecution in response to massively unfavorable publicity.⁷⁸ Thus, the public response to weak DMCA threats directed against scientific researchers serves as an effective check against such threats.

It is true, of course, that a truly determined plaintiff could threaten or file suit in spite of a weak substantive case and bad publicity, particularly if the plaintiff feels that the stakes are high (for example, where the copyright owner already has a large installed base of copyrighted works protected by the system at issue). Thus, academic researchers are not entirely insulated from the legal risk. However, the existence of some level of risk should not completely deter future research. Many activities raise the specter of legal risks; what is important is the magnitude of the risk in comparison to the benefits. As I have argued above, although the risk is

77. See McCullagh, *HP Backs Down*, *supra* note 50, at <http://news.com.com/2100-1023-947745.html>.

78. The government, in the end, decided to press ahead with the case, despite Adobe's withdrawal of support.

not zero, there are good reasons based both on the law and on practical realities surrounding DMCA litigation to believe that the risk is not so severe that encryption researchers should stop conducting research altogether, particularly given the importance of such research.

The basic message here is that under the appropriate circumstances, academic encryption researchers should not be afraid to conduct and publish certain forms of research. A common and quite reasonable response to new and uncertain legislation is to hunker down and avoid exposure to any risk of legal liability, or to focus on the flaws and ambiguities in the law. Although criticism of the ambiguous and imperfect aspects of the law is important, there is also a real risk that, by focusing so much on the possibility of liability, encryption researchers will wind up censoring themselves unnecessarily. If the government and private industry groups claim that these fears are unwarranted and exaggerated,⁷⁹ then researchers should take them at their word and begin vigorously exercising their rights within the framework laid out by the DMCA. Indeed, given that academic encryption researchers are in the best position to take advantage of the exemption (and given that non-academic researchers may be less able to do so), it is particularly important that such researchers not refrain from undertaking their research.

B. The DMCA Affects the Manner in Which Research Is Conducted

I have argued above that academic encryption researchers should be able to continue to conduct and publish certain types of research without significant risk of legal liability under the DMCA. This does not mean, however, that the DMCA is therefore unobjectionable. While it permits encryption research to continue, the DMCA has a significant impact on the conditions under which such research takes place. In many ways, the debate over whether encryption researchers will be civilly or criminally liable misses the point. The answer may well be no, but the more interesting and important question is whether the DMCA affects the way in which such research is conducted and whether this more subtle effect is problematic.

79. See, e.g., Dep't. of Justice Reply Br., *Felten* (No. CV-01-2669), available at http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011108_doj_reply_brief.html; Recording Indus. Assn. of Am. Mem. Supp. Mot. Dismiss, *Felten* (No. CV-01-2669), available at http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010712_riaa_mtd_memo.html; McCullagh, *Debunking DMCA Myths*, *supra* note 9, available at <http://news.com.com/2010-12-950229.html>.

As suggested above, I believe that the DMCA will have a non-trivial impact on the manner in which academic encryption research will be conducted. The impact comes from the steps that encryption researchers must take in order to avoid liability under the DMCA. The DMCA does not categorically exempt encryption research from liability. Instead, it places a number of conditions on the way such research is conducted. These conditions, while ostensibly inserted in order to sort “legitimate” from “illegitimate” encryption research, have the effect of influencing and regulating the behavior of academic encryption researchers.

First, and most critically, the DMCA will limit both the subjects of research and the universe of individuals permitted to conduct such research. As noted above, the exemption shields encryption researchers only from liability under § 1201(a) for access-control circumvention. It does not insulate researchers from liability under § 1202 for alteration of copyright management information, or under § 1201(b) for manufacturing technologies that circumvent rights-control technologies. Accordingly, researchers may well be precluded from researching such technologies. Furthermore, by privileging researchers with formal training or academic affiliations, the DMCA will prevent many existing researchers from engaging in such research.

Second, the DMCA raises a number of hurdles for a researcher to overcome before engaging in the research in the first place. One such hurdle is the need to obtain clearance for the research from the university or research organization and from legal counsel. To the extent that a researcher wishes to analyze an encrypted copyrighted work, the researcher would be well advised to obtain legal advice to ensure that the research is in compliance with the terms of the exemption. The department, university, or research organization may also have an interest in assessing its risk of liability for fostering such activities. Some university general counsel’s offices may have already developed policies for DMCA cases, but most others have not. This will involve a number of additional discussions and conversations.⁸⁰

Another initial hurdle will be to contact the copyright owner and make a good faith request for permission to engage in the act of circumvention. Failure to make such a request before engaging in the act of circumvention

80. Such discussions figured heavily in two cases I have been involved in. These discussions were particularly extensive in the *Felten* case, involving discussions with the general counsel offices of several universities, as well as private research organizations.

could, by the plain terms of the statute, make the exemption unavailable.⁸¹ Indeed, this is another reason why clearance with counsel is important. In many cases, researchers unaware of the exemption may undertake the act of circumvention before making the request; this requirement may thus be a trap for the unwary. And although nothing in the exemption suggests that a copyright owner's authorization is necessary before proceeding, the copyright owner may seek to suppress the research or influence its content,⁸² leading to additional conversations with counsel. Even if permission is eventually granted, there will be delays.

Third, the DMCA limits the universe of individuals with whom researchers can freely communicate about their research. One of the factors in the encryption research exemption focuses on the manner in which information derived from the encryption research is disseminated, i.e., whether in a manner reasonably calculated to advance the state of knowledge or in a manner that facilitates infringement. Before the DMCA, encryption researchers had few qualms discussing the results of their research, not only with academic colleagues, but also with the broader community of professional and amateur encryption researchers. As noted above, the encryption research community is characterized by much interaction between academic, professional, and "amateur" researchers. By disseminating information broadly, researchers obtain feedback and information about their research.⁸³ After the DMCA, however, a researcher must take care not to disclose weaknesses in encryption systems too broadly or too prematurely, since dissemination to the wrong set of individuals might constitute dissemination in a manner that facilitates infringement.⁸⁴

Fourth, the DMCA affects the avenues through which such information is distributed. Prior to the DMCA, encryption researchers, like other computer scientists, routinely made available information about their projects on the Internet, via email, on discussion boards, or through other

81. See, e.g., *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 320-21 (S.D.N.Y. 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

82. See, Compl. Declaratory J. and Injunctive Relief, *Felten* (No. CV-01-2669), at ¶¶ 41, 45-47 (No. CV-01-2669), available at http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html (technology and copyright owners asked for changes to be made in the research paper Felten's team was going to publish).

83. See Wagner Comment, *supra* note 31.

84. See, e.g., Elec. Frontier Found., *Researcher Escapes Chilling Effect of Digital Copyright Law*, at http://www.eff.org/IP/DMCA/20020808_eff_bunnie_pr.html (Aug. 8, 2002) (stating that the researcher refused to respond to emails from individuals with information regarding his attempts to crack the security in the Microsoft Xbox gaming console).

more informal channels. Again, the purpose was to encourage broad dissemination of information and subject it to critique and response as part of the scientific endeavor. After the DMCA, researchers may well prefer publication in more formal channels, such as academic journals, since this type of publication would better support a finding that the information was disseminated in a manner “reasonably calculated to advance the state of knowledge.”⁸⁵ Like the previous factor, the net effect here is to regulate and constrict the channels through which such information flows.

Fifth, just as the DMCA may constrict certain information flows, it forces other information flows. Prior to the DMCA, encryption researchers had no general obligation to seek permission for their research or to notify any third-parties of their results. The DMCA, however, now imposes both of these requirements, demanding that encryption researchers notify copyright holders of their intent to engage in research and requiring a good faith effort to seek authorization. In fact, this requirement is rather odd: if actual permission is required, then there is no need for an exemption. If, as is more likely, actual permission is not required, then why make the researcher ask for it?⁸⁶ The only reasonable explanation is to give the copyright owner notice of the research prior to its conduct.

In addition, the DMCA encourages disclosure of the research results to the copyright owners after the fact. In determining whether the exemption applies, a court is required to consider “whether the person provides the copyright owner of the work . . . notice of the findings and documentation of the research.”⁸⁷ Thus, the DMCA encourages not only giving notice of the research results, but also handing over the details of the research. Moreover, earlier disclosure would appear to be preferable, as the DMCA expressly directs courts to look at the timing of the disclosure. Thus, there may be pressure to disclose results prior to publication, and perhaps even during the course of the research.

Sixth, and perhaps most problematically, the DMCA may have a real effect on the content of research papers. As mentioned above, it is probably a stretch to apply the “tools” provisions of the DMCA to pure research papers that do no more than simply describe weaknesses in an implemented encryption system. However, as encryption researchers have repeatedly testified before Congress, the Copyright Office, and the courts,

85. 17 U.S.C. § 1201(g)(3)(A) (2000).

86. To see the tension between this requirement and the exemption, imagine a similar requirement in the copyright fair use context. For example, a requirement that anyone intending to write a book review first make a good faith attempt to seek authorization from the author for the quotes excerpted in the book review.

87. 17 U.S.C. § 1201(g)(3)(C).

researchers routinely use code in their papers to convey ideas and illustrate techniques. Moreover, they often distribute code to others for purposes of describing their methods and seeking verification of their results.

Any such code (whether source or, more troublingly, object) would look like a “technology” as it is defined under the tools provision. The encryption research exemption only permits distribution of “tools” to collaborators, not to the wider research community.⁸⁸ Although a researcher could still argue that the research paper overall is not “primarily designed . . . for the purpose of” circumvention,⁸⁹ it is difficult to gauge how courts would treat the code. It is quite possible that a court could consider the code to be “primarily designed” for circumvention, because after all, that is its literal purpose. Accordingly, a researcher might limit the amount of code disclosed in the paper and this might affect that researcher’s ability to convey ideas in the most effective and efficient manner.

Moreover, the overall structure of the encryption research exemption may have an impact on the content of research papers by involving copyright owners in the research process. The notice provisions give copyright owners an opportunity to ask for modifications of the paper in order to protect their economic interests. Indeed, in a number of cases, copyright owners have already asked for exactly these kinds of modifications.⁹⁰ A refusal to accede to “reasonable” requests for changes could be taken as a sign of lack of good faith. At the very least, this puts additional pressure on researchers to modify their papers in order to avoid trouble. The end result is that academic encryption researchers may not express themselves as freely as they would have absent the DMCA.

Thus, although academic encryption research can still occur under the DMCA, the DMCA will have a very real effect on the manner in which such research takes place. Moreover, this effect can be expected to slow the pace of discovery in this area. By limiting the subjects of research and the number of researchers, imposing additional hurdles before such research is undertaken, limiting the widespread dissemination of information, confining the avenues through which information is published, and affecting the content of published papers, the DMCA can be logically expected to raise the costs of engaging in such research. These additional barriers may be sufficiently high that some researchers may well choose to

88. *Id.* § 1201(g)(4).

89. *Id.* § 1201(a)(2)(A).

90. See Compl. Declaratory J. and Injunctive Relief, *Felten* (No. CV-01-2669), at ¶¶ 41, 45-47 (No. CV-01-2669), available at http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html.

pursue other topics, where there are no comparable hurdles.⁹¹ Thus, even though the actual risk of liability under the DMCA may be small, the regulation of the conditions of research may nevertheless hinder encryption research.

IV. A NORMATIVE ASSESSMENT OF THE DMCA'S IMPACT

Given the DMCA's effect on the conditions under which encryption research takes place, the next question becomes: Is it worth it? The fact that the DMCA regulates encryption research does not, by itself, make such regulation problematic. It could very well be that the costs borne by encryption researchers are justified by offsetting benefits. After all, one could argue that the DMCA's requirements are reasonable regulations that balance the need for research against the harm that research could cause to the economic interests of third parties such as copyright owners.

I will argue here that, for several reasons, the burdens on encryption research described above are not justified. In advancing this argument, I focus not on a precise and detailed measuring of the costs and benefits of such regulation. Instead, I challenge the underlying idea that we should be regulating encryption research in the first place. That is, I want to expand the scope of the inquiry and ask under what circumstances we should impose burdens on scientific research in order to protect intellectual property. I suggest that the circumstances should be extremely limited—certainly far more limited than currently provided under the DMCA.

What justifies the burdens the DMCA places on academic encryption researchers? The legislative history of the DMCA suggests that one possible justification is the need to sort “legitimate” from “illegitimate” encryption research.⁹² According to this justification, encryption research is extremely important and we must do everything to ensure that it can continue free and unabated. At the same time, there is a legitimate need to keep the encryption research exemption from being used as a loophole by

91. See, e.g., Wagner Comments, *supra* note 31.

92. House Commerce Report 511, *supra* note 27, at *47. The Report states:

The Committee recognizes that courts may be unfamiliar with encryption research and technology, and may have difficulty distinguishing between a legitimate encryption researcher and a so-called ‘hacker’ who seeks to cloak his activities with this defense. Section 102(g)(3) therefore contains a non-exclusive list of factors a court shall consider in determining whether a person properly qualifies for the encryption research defense.

Id. Aside from this brief mention, there are no other explanations for the specific conditions set forth in the exemption.

those who are primarily engaged not in research, but in copyright infringement. Under this view, some statutory limitations are necessary to prevent the use of the exemption as an illegitimate shield for piracy.

The problem with this justification is that the DMCA imposes far more burdens than necessary to accomplish this result. As already noted above, the DMCA does not merely sort “legitimate” from “illegitimate” research, leaving the “legitimate” research free to operate without constraint. Instead, it significantly regulates activities within the ambit of “legitimate” research. For example, the need to seek authorization from the copyright holder is hard to square with a pure “sorting” justification. Instead, it imposes an affirmative notice obligation upon researchers. The factor that encourages disclosure of research results to the copyright owner has a similar flavor. Both of these requirements do more than just help courts prevent abuse of the exemption—they regulate good faith encryption research itself.

Many other conditions in the encryption research exemption similarly have a significant impact on the activities of good faith encryption researchers. The DMCA imposes additional hurdles, which must be overcome before initiating the research. The exemption limits the scope of individuals with whom the researcher can freely communicate. It limits communication of the results of such research to certain channels and forces disclosure of information to others. Finally, it affects the content of what can be disclosed, preventing good faith researchers from communicating as freely and in as much detail as they would ordinarily like. Thus, the sorting rationale alone cannot be used to fully justify the impact the DMCA has on academic encryption research.

Given that this rationale appears insufficient, is there another way to justify the additional burdens the DMCA places on encryption research? One possibility is to argue that these burdens, whether intended or not, are justified because encryption research has the potential of harming the interests of copyright owners, and we want to permit the research but minimize the harm it causes. That is, by making available information about the weaknesses of deployed encryption systems, encryption research makes it more difficult for copyright owners to protect their works using this kind of technology. Accordingly, the DMCA effectively places a number of conditions (such as notice) on the manner in which such research takes place in order to reduce these impacts. The idea is thus not so

much to exempt good faith research entirely, but to balance the freedom to engage in such research against the interests of copyright holders.⁹³

Although this justification, unlike the sorting rationale, does provide a basis for imposing additional burdens on encryption research, it is a rather radical line of reasoning. To see just how radical, consider how copyright law currently treats the question of when to impose obligations on third parties to protect intellectual property rights. This issue of third-party obligations arises in the area of new technologies and the question of when the disseminators of such technology should be contributorily or vicariously liable for infringement. The Supreme Court addressed this issue in *Sony v. Universal City Studios*,⁹⁴ in the context of the VCR. More recently, cases such as *Napster*⁹⁵ and the ongoing litigation over other peer-to-peer file sharing networks⁹⁶ as well as other digital technologies such as SonicBlue's ReplayTV⁹⁷ also grapple with this difficult issue.

The concern expressed in many of these cases is balancing the need to combat copyright infringement with the fear of burdening the development of technologies with perhaps many other, non-infringing uses. Devices such as the ones mentioned above can be used to engage in copyright infringement. At the same time, they can be used for many legitimate purposes. Imposing liability on device manufacturers may reduce copyright infringement, but at the same time impose burdens on otherwise legitimate uses of the technology and on the development of technology generally. Copyright doctrine thus attempts to carefully sort out infringing from non-infringing uses, conscious of the potential impact of imposing liability one step removed from the actual infringement. Where to draw the line is a difficult question, and much has been written on the topic.⁹⁸

To the extent that we are concerned about the collateral impact of regulating the sale and marketing of technological devices that facilitate

93. Note that I am not arguing that Congress expressly thought of this justification. The legislative history actually contains very little explanation for the precise contours of the encryption research exemption. Instead, I am searching for potential justifications for these additional burdens.

94. *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

95. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

96. See, e.g., *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 243 F. Supp.2d 1073 (C.D. Cal. 2003).

97. See, e.g., *Paramount Pictures Corp. v. ReplayTV, Inc.*, No. CV 01-9358, 2002 WL 1301268 (C.D. Cal. Apr. 26, 2002).

98. See, e.g., Stacey Dogan, *Is Napster A VCR? The Implications of Sony for Napster and Other Internet Technologies*, 52 HASTINGS L.J. 939 (2001); Richard Gilbert & Michael Katz, *When Good Value Chains Go Bad: The Economics of Indirect Liability for Copyright Infringement*, 52 HASTINGS L.J. 961 (2001).

copyright infringement, we should be even more concerned about the collateral impact of regulating encryption research. This is because, in the context of encryption research, the DMCA does not regulate merely the infringing activity, or even the technological devices that may facilitate the infringing activity. Instead, the DMCA regulates the basic scientific research that may give rise to the technological devices that can be used to facilitate infringing activity. We are thus one step even *further* removed from the difficult cases involving the regulation of technological devices, and we are *many* steps removed from the actual act of infringement. Therefore, the DMCA represents a dramatic expansion of the regulatory impact of our copyright laws.

Because we are regulating activity that is so far removed from the actual infringing activity, we need to be exceptionally careful about the unintended or collateral effects of such regulation. As copyrighted materials have become increasingly more difficult to protect, copyright owners have taken ever more drastic steps to prevent infringement. The further upstream we move from the act of infringement, however, the more likely it is that unrelated downstream activities may be unfairly affected by such regulation. This is clearly a concern in the area of basic scientific research, which occupies a privileged position precisely because its downstream effects are difficult to predict.⁹⁹ A paper studying weaknesses in an implemented encryption system may be used to create a “black-box” used to pirate copyrighted works. That same paper may, however, also spur insights in other areas of encryption research, with significant applications in completely unrelated markets and industries. The basic point is that we need to be exceptionally wary in imposing any burdens on basic scientific research because we risk affecting potentially useful unforeseen downstream activities.

To be clear, I do not argue that science is holy and untouchable, and that any regulation of scientific research is improper. The government already regulates some areas of scientific research.¹⁰⁰ Indeed, the government has in the past (though not without controversy) restricted the dissemination of encryption research from the U.S. to other countries, in the course of controlling the export of technologies that might affect national

99. See, e.g., Steven Goldberg, *The Reluctant Embrace: Law and Science in America*, 75 GEO. L.J. 1341 (1987).

100. See, e.g., Atomic Energy Act of 1954, 42 U.S.C. § 2013 (1994 & Supp. V. 1999); *Bush Praises House for Human Cloning Ban*, CNN.COM (Feb. 27, 2003), at <http://www.cnn.com/2003/ALLPOLITICS/02/27/bush.human.cloning> (discussing proposed ban on human cloning).

security.¹⁰¹ Moreover, this particular type of research into implemented systems, though certainly academic, may be more intertwined with industry than other areas of pure, basic research. Thus, it would be a stretch to argue that encryption research should be categorically immune to regulation.

However, encryption research, like other basic scientific research, should only be regulated for good reason and with a properly cautious eye toward minimizing the potential collateral effects of the regulation. When the government regulates scientific research, it typically requires a significant justification, such as national security or public safety. The DMCA, by contrast, regulates research in order to protect the economic interests of third parties, namely copyright owners. Although these interests may be important, they do not rise up to the level of the other interests at stake when the government regulates scientific research. Moreover, as already detailed above, the DMCA, in pursuing this interest, does not regulate encryption research in a sufficiently careful manner.

Thus, I suggest that the government should be extremely cautious with regard to the impact of regulation on scientific research. In particular, it should be conscious of the potential downstream effects of regulation and properly sensitive to the fact that the future impact of research is difficult to predict. Accordingly, the government should carefully narrow regulation to address only the precise harm in question.¹⁰² The baseline assumption should be that research is fully privileged. Unfortunately, in the context of the DMCA, the attitude toward encryption research has not evinced any of these careful qualities.

It is interesting to speculate about why the DMCA does not reflect this kind of careful consideration of the potential impact on scientific research. Part of the reason may simply be that Congress was not well equipped to fully appreciate the unique nature of encryption research. Encryption researchers were initially unaware of the effect that the proposed DMCA

101. See, e.g., *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000); Matthew Parker Voors, *Encryption Regulation In The Wake Of September 11, 2001: Must We Protect National Security At The Expense Of The Economy?*, 55 FED. COMM. L.J. 331, 344-45 (2003); Tricia E. Black, Note, *Taking Account of the World As It Will Be: The Shifting Course of U.S. Encryption Policy*, 53 Fed. Comm. L.J. 289, 298 (2001).

102. Ideally, the regulation should also build in some flexibility to permit either courts or the Copyright Office to minimize these collateral effects as they are discovered. The DMCA does not adopt this approach, preferring instead to provide narrow, statutory exemptions. And although Congress did direct the Copyright Office to report back on the impact of the DMCA on encryption research, the timing of the report (before the effective date of the relevant DMCA provisions) suggests that Congress did not view this as a serious mechanism for generating modifications to the DMCA.

would have on their activities, and were thus late in lobbying for an exemption. Moreover, unlike other areas of scientific research, which are typically regulated by expert agencies, encryption research in the context of the DMCA did not benefit from the input of scientists within the regulatory process. Thus, despite ample testimony from encryption researchers, Congress may not have fully appreciated how the DMCA might affect such research.

Another possible explanation arises from different conceptual frameworks for information circulation. The DMCA views information as a resource to be controlled. In supporting such control, the DMCA seeks to limit circulation of information that would facilitate circumvention of technological protection measures. In this light, some limits on the circulation of scientific information might not appear to be onerous. Yet the culture of scientific research reflects a very different view of information circulation. This culture generally supports—and indeed relies upon—the free and easy circulation of information, and actively resists efforts to limit such circulation.¹⁰³ Thus, barriers on information flow that might not faze the private entities accustomed to protecting information may cause significant disruption to academic communities that rely heavily upon free circulation of information.

A simple analogy from a different context highlights the problematic impact of the DMCA on scientific research. Imagine that a company manufactures and sells bicycle locks. After years of research, the company invents a new metal alloy that is both strong and lightweight and uses this new alloy on its new locks. These locks are immensely successful. The company sells hundreds of thousands of them, and people throughout the country use them to secure bikes. A professor of materials science decides to study the properties of this new alloy, as implemented in the bike lock. She discovers that a simple combination of household chemicals, when applied to the lock, dramatically weakens it, making it easily breakable. Publication of these results would enable individuals to easily circumvent the protection offered by the locks and effectively destroy the market for these locks.¹⁰⁴

103. See, e.g., Rebecca Eisenberg, *Proprietary Rights and the Norms of Science in Biotechnology Research*, 97 YALE L.J. 177, 183-84 (1987); Harold P. Green, *The Law-Science Interface in Public Policy Decisionmaking*, 51 OHIO ST. L.J. 375 (1990). Of course, this has been changing in recent years, as the line between university and industry research has been blurring. See, e.g., Eisenberg, *supra*; Arti Rai, *Regulating Scientific Research: Intellectual Property Rights and the Norms of Science*, 94 NW. U. L. REV. 77 (1999).

104. A real-life analog of this hypothetical can be found in Matt Blaze's recent discovery of weaknesses in mechanical lock systems based on a master key. See Matt Blaze,

What conditions should we properly place on the scientist's research and the publication of the results of the research? Would it be appropriate to impose a requirement that the scientist ask permission from the lock maker, before engaging in her research? Would it be appropriate to require disclosure of the research and results to the lock maker? To limit such research to those who have training in materials science and are affiliated with a research institution? To require that information about the weaknesses in the lock be published only in certain academic fora, but not, say, on the Internet or on an electronic bulletin board?

Many, I believe, would instinctively resist the imposition of any of these conditions upon this research. It is not difficult to see why. First, we understand the general importance of this kind of scientific investigation. Using this analogy, it is somehow easier to see that this type of research is *basic* research. It leads to the creation of important knowledge and thus should be encouraged and disseminated widely. Second, we recognize that limiting dissemination of this kind of knowledge may be harmful. Other individuals and scientists should know about the weaknesses in the alloy as soon as possible so that no one uses it for its strength without realizing this fatal defect.

Third, there is the impropriety of imposing restrictions on an unrelated third party who is pursuing knowledge. Why should we charge the researcher with the task of providing notice of her results to a private company? Why should we subject her to limits regarding to whom she can talk about her research? Fourth, and relatedly, there is a sense that the blame for the harm should rest not on the researcher, but on the company for relying upon a material that later proves to be faulty. Why should the law protect the poor technological choices by regulating the dissemination of research?

Finally, the example highlights the fact that liability for the undesirable activity should be, to the greatest extent possible, limited to the actual undesirable activity rather than to the scientific research that may enable it. It is true that publication of the research may result in some harm, as someone might use the information to break locks and steal bikes. The proper response, however, is not to regulate the creation and dissemination of the information, since this will have significant undesirable collateral effects and may ultimately result in less security. Rather, the proper response is to regulate the harm directly. Thus, it should be illegal (as it is)

Cryptology and Physical Security: Rights Amplification in Master Keyed Mechanical Locks, 1 IEEE SECURITY AND PRIVACY (forthcoming Mar./Apr. 2003), available at <http://www.crypto.com/papers/mk.pdf> (last visited May 5, 2003); see also John Schwartz, *Many Locks All Too Easy to Get Past*, N.Y. TIMES, Jan. 23, 2003, at C1.

to use the information to break a lock and steal a bike. Perhaps it should even be illegal to sell a “lock breaking” kit, although there might be many good reasons to provide such a kit. Certainly, however, it should not be illegal to publish basic research about weaknesses in the alloy without first jumping through many regulatory hoops. Even the placement of minimal conditions on such research seems inappropriate.

As with all analogies, there are limits, distinctions, and ways in which this analogy is not perfect. Yet I believe it captures in a concrete way what is going on in the field of encryption research under the DMCA. The DMCA regulates the conduct of basic scientific research to the benefit of private parties who *might* be adversely affected by uses of such research. The example above illustrates precisely why we should think hard before imposing even minimal burdens on basic scientific research in support of the private economic interests of unrelated third parties.

V. POTENTIAL LEGAL RESPONSES

In light of the above analysis, the DMCA should exempt, to the maximum extent possible, encryption research from liability. Instead of imposing conditions on such research, the DMCA should focus more narrowly on uses of such research that directly facilitate or encourage acts of infringement. The basic goal should be to eliminate, as much as possible, any impediments to the conduct and publication of research and focus more carefully on the precise harms at issue. In so doing, the DMCA could appropriately distinguish legitimate research from illegitimate attempts to use research as a cover for infringing activity. But the DMCA should be far more careful about doing so in a way that does not burden actual research.

There are several ways to achieve this goal. One way is through expansive judicial interpretation of the exemption, in light of the concerns expressed in this Article. For example, a liberal interpretation of the “good faith” notice requirement would reduce the burden of seeking prior authorization. In cases where the researcher, in good faith, did not know about the requirement or found the requirement too burdensome to satisfy, courts should be quick to excuse the failure and not withhold the exemption entirely. Similarly, courts should not take the failure to comply with the copyright owner’s editing requests as evidence of a lack of good faith.

A court might also broadly interpret the overall good faith requirement so that it is consistent with existing encryption research practices. In determining whether research is being conducted in good faith, courts should take notice of the realities of scientific research in this field. In particular,

courts should read the “training” requirement to encompass both formal and informal types of training. Courts should also read broadly the “manner of dissemination” to acknowledge that encryption researchers often post information on websites and in other fora outside of traditional publication. This would minimize the burden on the free circulation of information within the encryption research community.

Finally, the courts should interpret the tools provisions narrowly to permit encryption researchers to exchange and publish information about their discoveries in the manner to which they have traditionally been accustomed. Thus, publication of a description should certainly be privileged. Furthermore, publication of source code, or even object code, should not violate the tools provision, insofar as the “purpose” of such publication is not to facilitate circumvention, but rather to enlarge the scope of knowledge. Such an interpretation will permit encryption researchers to communicate information about their research in the most efficient way.

If the courts were to interpret the DMCA in the fashion suggested here, the regulatory burden on encryption researchers would be greatly reduced (although not entirely eliminated).¹⁰⁵ Moreover, this interpretation is more in line with the stated purpose of the exemption, namely to distinguish between “legitimate” and “illegitimate” encryption research. The courts should use the standards within the research community to measure what is “legitimate” research, and once determined to be legitimate, the research should be subject to little or no regulation. Researchers should be able to disseminate information about their discoveries as broadly as possible (even if this might have the effect of harming the economic interests of intellectual property holders) without fear of liability. If the purpose of the exemption is to ensure that “good faith” encryption research can continue unfettered (rather than be regulated to protect the interests of third parties), then the suggested approach would be superior. Courts would then be truly limited to policing attempts to invoke the exemption for improper reasons.

The problem with the above approach is that it is unlikely to be implemented. For the reasons set forth in the earlier part of this Article, it is unlikely that a case involving an academic encryption researcher will be fully litigated in the above fashion. Copyright owners are reluctant to bring suit in the context of academic encryption research. Accordingly, a

105. For example, the concern about liability under § 1202 for altering copyright management information would still remain.

clarifying set of interpretations will probably not be forthcoming anytime soon.

Therefore, a better approach would be to craft a broader exemption under the DMCA for encryption research, one that gives maximum freedom to encryption researchers. A bill proposed by Senator Boucher contains such an exemption.¹⁰⁶ It would amend the anti-circumvention provisions of the DMCA to permit otherwise prohibited conduct when engaged “solely in furtherance of scientific research into technological protection measures.”¹⁰⁷ As proposed, the exemption would provide a much broader exemption for scientific research, in addition to placing fewer restrictions on the conduct of research.¹⁰⁸ This kind of broad exemption would do a superior job of ensuring that basic scientific research is left unaffected by the DMCA.

VI. CONCLUSION

This Article has discussed a narrow—but important—issue. The world of academic encryption researchers represents a small and specific slice of the broader population affected by the DMCA. Thus, it would be tempting to dismiss concerns about laws that affect only this small slice of the population. Yet laws that raise additional barriers to scientific inquiry have the potential to affect a great many individuals who benefit from scientific discoveries. Studying the impact of the DMCA on this group of scientists illustrates how far the DMCA reaches in its attempt to protect private intellectual property rights and highlights concerns about the collateral impact of our intellectual property laws.

106. See Digital Media Consumers' Rights Act of 2002 (DMCRA), H.R. 5544, 107th Cong. § 5 (2002), available at <http://www.arl.org/info/frn/copy/copytoc.html>.

107. *Id.*

108. This kind of amendment has also received support from the IEEE and from Richard Clarke, the former cybersecurity “czar” for President Bush. See *IEEE-USA Position Statement: Digital Millennium Copyright Act (DMCA) Encryption Research*, at <http://www.ieeeusa.org/forum/POSITIONS/DMCAencryption.html> (June 20, 2002).

