Submission of Edward W. Felten
Associate Professor of Computer Science, Princeton University

Library of Congress / Copyright Office Rulemaking on "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies"

Classes of Works

I ask the Librarian of Congress for an exemption for the following class of works:

(1) Musical recordings and audiovisual works, protected by access control mechanisms whose circumvention is reasonably necessary to carry out a legitimate research project, where the granted exemption applies only to acts of circumvention whose primary purpose is to further a legitimate research project.

Should the Librarian conclude that the above Class 1 does not constitute a valid "class of works" as defined in the Notice of Inquiry (NOI), I ask the Librarian to grant in the alternative an exemption for the following class of works:

(2) Musical recordings and audiovisual works, protected by access control mechanisms whose circumvention is reasonably necessary to carry out a legitimate research project.

Summary of Argument

The requested exemption would enable legitimate research relating to access control technologies. At present, much research of this type is impossible due to the prohibition on acts of circumvention in 1201(a)(1). The requested exemption would allow this research to proceed.

The current state of the art in access control technology is due in large part to past research on those technologies. Yet today's state of the art does not provide the desired level of protection for copyrighted content, so future research is needed. Without an exemption for legitimate research, much of the needed research will not occur.

The requested exemption is not limited to encryption research but would cover all of the legitimate access control research that is being prevented by 1201(a)(1).

My account of the harms caused by 1201(a)(1) – harms that would continue to accrue absent an exemption – is based in part on my direct personal experience in performing access control research prior to the effective date of 1201(a)(1), and on my personal plans to resume such research should an exemption be granted. My account is also based on my general knowledge about my colleagues in the computer security research community, and my colleagues in other scholarly fields.

I realize that the Librarian might conclude that it is impossible, within the confines of the NOI to grant an exemption for legitimate research. The Librarian might, for example, reach such a conclusion based on a determination that the NOI does not allow the Librarian to create an exemption that is narrowly tailored to enable legitimate research. If the Librarian does conclude that the NOI does not allow an exemption to protect legitimate research, I ask the Librarian to state that conclusion clearly, so that it is clear that any legitimate-research exception to 1201(a)(1) would require Congressional action.

Scope of The Request

I ask the Librarian to create an exemption that will protect the ability of legitimate researchers to carry out their research. If it is possible for the Librarian to grant an exemption that applies only to acts of circumvention whose purpose is to advance legitimate research, then I ask the Librarian to grant such an exemption. If such an exemption is not possible, then I request the narrowest possible exemption that both (a) is a "class of works" under the NOI, and (b) exempts all legitimate research.

The first class of works for which I request an exemption is designed to exempt only legitimate research:

> [Class 1:] Musical recordings and audiovisual works, protected by access control mechanisms whose circumvention is reasonably necessary to carry out a legitimate research project, where the granted exemption applies

only to acts of circumvention whose primary purpose is to further a legitimate research project.

I believe that this is the narrowest possible exemption that would unshackle legitimate research.

I recognize that the Librarian may find that Class 1 does not meet the criteria for a "class of works" under NOI. If that finding is made, I ask the Librarian to consider my second proposed class of works, which is simpler but broader than the first:

> [Class 2:] Musical recordings and audiovisual works, protected by access control mechanisms whose circumvention is reasonably necessary to carry out a legitimate research project.

I note that in the 1999 rulemaking, the Librarian granted an exemption for a class of works, protected by access control technologies that had a certain attribute. This exemption covered "Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsoleteness." Based on this precedent, I believe that the proposed Class 2 likely is a viable "class of works." However, I recognize that the Librarian may find otherwise.

Evidence of Actual Harm and Likely Future Harm

The prohibition on acts of circumvention in 1201(a)(1) has caused harm, and will continue to cause harm, by preventing legitimate research that would benefit the public and would lead to a better understanding of the capabilities and limitations of access control technology and other critical computer security technologies.

My assertion that 1201(a)(1) is preventing research is based in part on my direct personal experience. Before 1201(a)(1) went into effect, my colleagues and I performed access control technology research that would have been impacted by 1201(a)(1). I halted that research program when 1201(a)(1) went into affect. I intend to resume that research program if the requested exemption is granted.

One example of the kind of work affected by 1201(a)(1) is research on digital watermarking of recorded music, and related technologies, that my colleagues and I

performed in the fall of 2000. We studied six separate technologies for controlling access to digital music, including four watermarking technologies and two others. This research led to the publication of a widely acclaimed paper:

> Reading Between the Lines: Lessons from the SDMI Challenge. Scott A. Craver, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan W. Wallach, Drew Dean, and Edward W. Felten. Proceedings of the 10th USENIX Security Symposium, August 2001. Available at http://www.usenix.org/events/sec01/craver.pdf.

Although this paper was published after the effective date of 1201(a)(1), all of the research described in it, including the acts of circumvention, occurred before 1201(a)(1) took effect. (This paper led to a Federal lawsuit involving DMCA provisions other than 1201(a)(1).) It is not currently possible to continue this line of research, as continued work in this area would run afoul of 1201(a)(1). Research would be able to resume if the requested exemption is granted.

My assertion of harm is also based on my knowledge about the research programs and plans of my colleagues throughout the computer security research community. Independent research of the sort that would be covered by the requested exemption was (obviously) halted in the United States when 1201(a)(1) went into effect, and to my knowledge there is no such independent research going on in the United States today. This was an area in which the United States had been one of the world leaders.

I am Program Chair for the 2003 ACM[1] Workshop on Digital Rights Management, which is one of the leading venues for publishing the kind of legitimate research that 1201(a)(1) bans. (As Program Chair, my job is to manage and oversee the process of soliciting, reviewing, and selecting papers for presentation at the Workshop.) As Program Chair of this Workshop, I am convinced that, absent the requested exemption, the technical quality and variety of papers published at the Workshop will suffer because of 1201(a)(1).

---

[1] ACM, the Association for Computing Machinery, is the leading international professional society for computer scientists.

Chilling Effect of 1201(a)(1) on Other Research

It is worth noting that the harm caused by 1201(a)(1) extends even to research that might ultimately be found to be beyond the literal scope of 1201(a)(1). This is due to at least two factors.

First, there is considerable uncertainty about how the distinction is drawn between access control technologies (covered by 1201(a)(1)) and technologies designed to protect the rights of copyright holders. It is not clear whether the DMCA intends these categories to be distinct or whether they can overlap. In any case, researchers find this distinction confusing and doubt its technical validity. Common usage tends to equate access control with copy control; for example the CSS access control technology for DVDs is licensed by a body called the DVD *Copy Control* Association. I also note that the Librarian has remarked on the vagueness of this distinction. The chilling effect of this uncertainty on prudent researchers is considerable.

Second, when researchers are choosing whether to start a research project, they often lack the information needed to determine whether the research will later be entangled by 1201(a)(1). In my experience, half or more of the effort in an access control research project is spent in characterizing how the subject technology works. It is only after this characterization is complete that the researcher has the information needed to determine whether completing the research project is impossible due to 1201(a)(1). When a researcher cannot tell *a priori* whether the time and resources spent on a project will ultimately be wasted due to 1201(a)(1), he will naturally shy away from performing such research.

In short, 1201(a)(1) does more than simply banning one category of research. It also makes research in related areas riskier. The requested exemption would eliminate this risk, and thereby increase research activity in these related areas.

Existing Exemptions are Not Sufficient

The existing statutory exemptions to 1201(a)(1) do not obviate the need for the requested exemption, because they do not protect much of the relevant research.

The exemption for nonprofit libraries, archives, and educational institutions applies only to very limited circumstances involving purchasing decisions. It does not protect access control research.

The exemption for reverse engineering similarly applies only to limited circumstances in which the sole purpose of the circumvention is to create an interoperable program. Access control researchers have other (legitimate) purposes, so this exemption will not protect them.

The exemption for encryption research does protect some research, but it does not protect research that is unrelated to encryption. Encryption, as that term is defined in the statute and used by technical experts, is *only one* of the methods employed by access control technologies, so this exemption can protect a researcher only if the access control technology he is studying happens to employ encryption. (Non-experts often mistakenly conflate encryption with access control, but the two are not the same.) For example, at least four of the six technologies studied in the paper referenced above were non-encryption technologies. Thus the encryption research exemption does not obviate the need for the requested exemption.

Benefits of Access Control Research

Research on access control technologies provides many benefits to the public and to copyright holders. Research advances the knowledge of all parties, thereby allowing them to make better decisions. Research gives consumers more information about the implications of access control technology for their lawful use of protected works, thereby helping consumers to make more informed and more confident purchasing decisions. Research gives copyright owners a better understanding of the capabilities and limitations of the technologies available to them, so that they can make better decisions about whether to entrust their content to those technologies.

Research fosters an informed public debate about legislative and regulatory proposals that would mandate the use of access control or other "digital rights management" technologies in future media devices.

I note that the requested exemptions apply only to *legitimate* research. Antisocial acts whose primary aim is to cause infringement are not legitimate research and would not be protected.

The Librarian's Analysis of My Request

To facilitate the Librarian's consideration of my request, I respectfully suggest that the Librarian use the following procedure for evaluating my request.

I ask the Librarian to consider first whether legitimate research on access control technologies, considered as a whole, is beneficial or harmful to the public. If the Librarian determines that this category of legitimate scholarship is harmful to the public, then the Librarian should reject my request for that reason.

Assuming that the Librarian finds legitimate access control research to be beneficial to the public, I ask the Librarian to consider next whether Class 1 is a valid class of works under the NOI. If the Librarian determines that Class 1 is a valid class of works, then the Librarian should grant an exemption for Class 1. Since Class 1 is defined so that the *only* effect of granting an exemption for it is to enable legitimate research, and since (by assumption) the Librarian had decided that enabling such research would benefit the public, the exemption would be justified.

If the Librarian finds that Class 1 is not a valid class of works, I ask the Librarian to consider next whether Class 2 is a valid class of works under the NOI. If Class 2 is not a valid class of works, then the Librarian should reject my request on the grounds that neither of the requested class of works is valid under the NOI.

Analyzing Class 2 (If Necessary)

Assuming that the Librarian has found that legitimate research benefits the public and that Class 2 is a valid class of works, I ask the Librarian to consider next whether the

overall effect of exempting Class 2 would be beneficial or harmful to the public. This is a more complex inquiry.

A Class 2 exemption would have two effects. First, legitimate research would be enabled. By assumption, this would benefit the public. Second, anyone would be allowed to circumvent any access control technology for any reason, provided only that that technology was a potential subject of legitimate access control research. Many of these non-research circumventions would probably be considered harmful, at least under the assumptions inherent in the NOI, so it seems very likely that the Librarian will conclude that these non-research circumventions, considered as a whole, would be harmful to the public.

If the Librarian finds that these non-research circumventions are beneficial, then the Librarian should grant an exemption for Class 2, since that exemption would benefit the public.

If the Librarian finds, as seems likely, that the overall effect of non-research circumventions would be harmful, then the question becomes whether those harms outweigh the benefits of enabling legitimate research. If the harms of non-research circumvention outweigh the benefits of research, then the Librarian should reject my request, on the grounds that the Librarian cannot offer an exemption narrowly tailored for legitimate research, and the non-research harms of a broader Class 2 exemption outweigh the research benefits. If, on the other hand, the Librarian finds that the benefits to the public of research outweigh the harms due to non-research circumvention, then the Librarian should grant an exemption for Class 2, on the grounds that the exemption is allowable within the NOI and benefits the public.

Concluding Remarks

As the Librarian is doubtless aware, the limitations on research imposed by 1201(a)(1) (not to mention other parts of the Digital Millennium Copyright Act) are of serious concern for the legitimate research community. Even if no exemption is granted, the Librarian can help legitimate researchers – and everyone else – by delineating clearly the reasoning used in responding to researchers' requests, and especially by shedding

light on whether an exemption for legitimate, beneficial research is even feasible within the limited rulemaking process authorized by Congress.

I thank the Librarian for the time and effort spent on considering this request.

Contact information:

Edward W. Felten
Dept. of Computer Science
Princeton University
35 Olden Street
Princeton, NJ 08544
(609) 258-5906 voice
(609) 258-1771 fax
felten@cs.princeton.edu