Statement of Barbara Simons
Co-Chair of USACM

The U.S. Public Policy Committee of
The Association For Computing Machinery (USACM)

Before the Copyright Office of the Library of Congress Regarding The Need for Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

May 14, 2003

Good morning Ms. Peters and distinguished representatives of the Copyright Office. Thank you for the opportunity to testify at this important hearing as part of the Copyright Office's anti-circumvention rulemaking proceeding.

I am co-chair of USACM, the U.S. Public Policy Committee of the Association for Computing Machinery. ACM is the leading non-profit educational and scientific computing society of nearly 75,000 computer scientists, educators, and other information technology professionals committed to the open interchange of information concerning computing and related disciplines. ACM is also a publisher, with a large on-line digital library.

USACM (which I founded in 1993) serves the ACM membership and community by providing policymakers, courts, and the public with a deeper understanding of computer and Internet issues and their convergence with legislative and regulatory initiatives.

I am a Fellow of ACM and of the American Association for the Advancement of Science, and formerly served as the President of ACM and Secretary of the Council of Scientific Society Presidents. I earned my Ph.D. in computer science from U.C. Berkeley, worked at IBM Research for many years and have authored numerous technical papers. I have been a consulting professor at the University of California, Santa Cruz, and Stanford University.

My statement today represents the views of the USACM. To underscore the importance of this rulemaking proceeding to the computing community, my statement has also been endorsed by the Computing Research Association - an association of more than 180 North American academic departments of computer science and computer engineering, industrial and academic laboratories, and affiliated professional societies.

USACM Findings

USACM has found section 1201 of the DMCA to have substantial negative impacts on the conduct of basic research in the U.S., particularly in cryptography and other computer security areas. The section interferes with many legal, non-infringing uses of digital computing and prevents scientists and technologists from circumventing access technologies in order to recognize shortcomings in security systems, to defend patents and copyrights, to discover and fix dangerous bugs in code, and to conduct forms of desired educational activities.

Examples of Legitimate Activities Prohibited by Section 1201

The following are just a few illustrations of legitimate activities currently prohibited by section 1201:

*A financial institution receives a digital object protected by code obfuscation using means other than encryption. Employees of the firm suspect it contains a highly destructive computer virus or worm. The only way to find out if these suspicions are valid is to circumvent the obfuscation techniques to see what the code actually does. Because the code -- including a possible virus -- qualifies as an "original work of authorship," the act of its circumvention is prohibited.

* A contractor employs software technology from a third party in a system widely used by law enforcement. In the course of use, a serious flaw ("bug") is discovered that makes the system fail unexpectedly. The third party could be unresponsive. Or, worse yet, the third party could be suspected of being a "front" for a crime organization not trusted to provide a fix for the software. Whatever the case, because the software is protected as an original work of authorship, no reverse engineering or circumvention is allowed to fix the flaw in a trusted manner.

*A firm wants to test a computer system before purchasing it to ensure that it is trustworthy and secure or to check for patent and licensing violations in the code itself. Circumventing a technical measure without the producer's permission is prohibited.

*Scientists and educators are prohibited from teaching many of the standard security techniques to investigate security risks, because these same techniques can be employed to circumvent copyright protection mechanisms.

*A copyright owner might suspect that a user is infringing his work. The only way to test his assumptions is to bypass the encryption scheme of the suspected work to assess the material. Bypassing the encryption scheme is prohibited.

ACM Declaration in the Felten Case:

I would like to quote from a portion of ACM's declaration in the Felten et al v. RIAA et al case, a copy of which is included in the packets we have provided. The concerns we expressed in that document in 2001 remain all too relevant today.

<u>Application of the DMCA to the Presentation and Publication of Research Would be Harmful to Science</u>

13. Research in analysis (i.e., the evaluation of the strengths and weaknesses of computer systems) is essential to the development of effective security, both for works protected by copyright law and for information in general. Such research can progress only through the open publication and exchange of complete scientific results.

14. ACM is concerned that Sections 1201 to 1204 of the Digital Millennium Copyright Act (hereinafter these Sections will be referred to as the "DMCA") will have a chilling effect on analysis, research, and publication, as the result of litigation itself or of the threat of or concern about potential litigation.

15. ACM is also concerned that application of the DMCA to the presentation and publication of scientific papers could result in the departure from the U.S. of the information security community for conferences and publications. If conference organizers cannot afford to take the risk of publishing papers, such as the papers that ACM expects will be submitted for its November 5 [2001] workshop as described below, those conferences may be held in other countries where the risk of liability is lower. Such a result would have a negative impact on this country's leadership in research in that area.

The Upcoming Digital Rights Management Workshop

16. ACM is particularly concerned about the potential implications of the DMCA for its [then upcoming] November 5, 2001 Workshop on Security and Privacy in Digital Rights Management (the "DRM Workshop").

17. ACM's description of the workshop states:

> "This workshop will consider technical problems faced by rights holders (who seek to protect their intellectual property rights) and end consumers (who seek to protect their privacy and to preserve access they now enjoy in traditional media under existing copyright law).
>
> "Digital Rights Management (DRM) systems are supposed to serve mass markets, in which the participants have conflicting goals and cannot be fully trusted. This adversarial situation introduces interesting new twists on classical problems studied in cryptology and security research, such as key management and access control.
>
> "The workshop seeks submissions from academia and industry presenting novel research on all theoretical and practical aspects of DRM, as well as experimental studies of fielded systems."

18. The DRM Workshop is accepting research papers on a number of topics that are potentially restricted by the DMCA, including access control mechanisms, architectures for Digital Rights Management ("DRM") systems, broadcast encryption, electronic

commerce protocols, encryption and authentication for multimedia data, key management in DRM systems, portability of digital rights, privacy and anonymity, privacy-preserving data mining, robust identification of digital content, tamper resistant hardware and consumer devices, threat and vulnerability assessment, and watermarking and fingerprinting for media software.

19. Like many other ACM workshops, ACM plans to publish the papers accepted for the DRM Workshop as Proceedings. ACM is concerned that the publication and presentation of technical papers on many of these topics, especially papers on watermarks, encryption, authentication, access control systems, tamper resistance, and threat and vulnerability assessment, could raise problems under the DMCA. We are concerned that ACM, along with its conference and workshop organizers and member authors, will be open to the same threats and run the same risk of legal liability as were Professor Felten, his co-authors and the organizers of the Information Hiding Workshop.

20. ACM is also likely to sponsor other conferences that may be affected by the DMCA. Virtually all conferences that discuss the security of digital information may be subject to threats under the DMCA because such conferences consider the strengths and weaknesses of various technological protection measures that could be applied, or are actually being applied, to protect copyrighted works.

Harm to ACM and Its Members

21. ACM has earned the reputation of choosing strong scientific papers through a peer review process without regard to political or commercial pressure. Its reputation as a leading scientific and technical organization could be substantially damaged within the scientific and technical community if it were to fail to publish a properly submitted and peer-reviewed paper because of commercial pressure or the fear of litigation.

22. Any restriction that the DMCA may impose on the publication of scientific research will keep foreign researchers from attending our conferences in the United States, with the potential loss to ACM of members and of revenue from memberships, conference participation, and publications.

23. Because the DMCA is a new statute and its application to scientific research is unclear, ACM cannot accurately assess the risk involved in presenting and publishing papers on computer security and on technologies used to protect copyrighted digital works. Even if ACM were willing to assume whatever risk were involved in the presentation and publication of such papers, our members may not. We are concerned that some of our members, intentionally or not, may censor their submissions to avoid potential DMCA problems. If that were to happen, the quality of ACM papers and presentations would be hurt and the scientific community as a whole could suffer substantial damage.

The DMCA Poses a Continuing Problem

24.Beyond the possibility of DMCA problems at the November DRM Workshop, ACM may continue to face potential problems in the future. ACM has long published papers in fields addressing the circumvention of security and technical protection measures. Unbiased, objective research in the field of computer and data security has always included research into the weaknesses as well as strengths of security measures. ACM could adopt a policy of steering clear of papers that could subject it to liability under the DMCA, but that could only be done at the risk of sacrificing its mission and damaging its reputation as a scientific organization.

25. In sum, as long as Sections 1201 to 1204 of the DMCA could be interpreted to reach scientific and technical publications, ACM and its members are concerned that they will face a continuing risk of litigation and liability.

Chilling effects – Personal experiences

Unfortunately, the concerns ACM expressed in the Felten declaration, quoted above, are no longer hypothetical. A few days ago in preparation for this testimony, I posted a note to USACM requesting personal experiences from people who had had problems with the anti-circumvention provisions of the DMCA. I received three responses on 5/8/03, all of which are quoted below with permission.

One of the people with whom I communicated is Dutch computer scientist Niels Ferguson. Ferguson withdrew a paper detailing weaknesses in the HDCP content protection system from the ACM DRM Workshop referred to in the ACM declaration, and instead wrote a paper entitled, “Censorship in Action: Why I don’t Publish my HDCP Results”. That paper is included in your packet. He also made the following comment in email.

> Since my experiences with my HDCP paper I have stopped doing research on the security of cryptographic systems that protect copyrights. There is no point in doing research if I can't publish my results. I have spoken to several other experienced cryptographers, and many have come to a similar conclusion.
>
> Of course, this lack of research almost guarantees that the copyright-protection techniques will be easy to break, and that works will be pirated for years to come. We know from experience that systems designed without public review are almost always weak. Without public review, there is no security. And without security, the pirates will thrive.

A second communication was from Prof. Dr. Andreas Pfitzmann, of the Technische Universitaet in Dresden. Prof. Pfitzmann was on the program committee of the Information Hiding Workshop at which Prof. Felten was supposed to have presented his paper initially:

> I do not know how much inside knowledge you have about the Felton case, which started at the Information Hiding Workshop which accepted that paper for presentation, where not only Felton and his co-workers, but also PC [Program Committee]-chair Ira Moskowitz (Cc) and General Chair John McHugh (Cc) have been threatened personally. In the latter case, the employer was willing to take the legal risk.
>
> Finally, it was mostly the European members of the PC who voted to NOT exercise any influence whether to present or not to present that accepted paper, but to leave that decision completely to the authors. And it was the decision to let no American chair the session scheduled for the Felton paper, but a European citizen - me.
>
> For the Workshop, it worked out very well in the end by a lot of publicity (and probably this paper got even during the workshop so many readers as no other paper), but when accepting to chair that session - when I did not know whether the paper would be presented or not - it was quite clear to me that this could mean staying in the US for quite a while. Since I am working as an advisor for the German government concerning privacy and security, I was quite optimistic that it would work out well in any case for me personally, since I expected so much help by Germany and the EU as could be, but it looks somehow strange that mainly the Europeans were in charge of helping to maintain basic liberties, e.g. to speak about the freedom to discuss research, in the US.
>
> After experiencing the threat to the Information Hiding Workshop mentioned above, I would argue to exempt the organizers, PCs and session chairs as well as publishers of scientific conferences and workshops.
>
> As long as this is not done, we decided to avoid the US for the Information Hiding Workshop and I personally successfully argued to hold the successor of PET 2003 not in the US, but Canada.
>
> In addition, it caused me to argue to stay with Springer Verlag (Germany) as the publisher and not to switch to ACM with regard to PET 2004 (we stayed with Springer with regard to Information Hiding Workshop without any discussion), as we want to stay away from US jurisdiction as far as possible.

The third communication was from Prof. David Wagner, who is in the Computer Science Department at U.C. Berkeley:

> We looked at HDCP, a copy protection system destined for use in (I'm told) high-definition TV sets. We very quickly found that it had serious security flaws. We wrote a paper and submitted it to a scientific workshop. Then, we realized that we were running right down the same path the Felten group did, and hey, we'd better be careful! I then spent the next month or two conferring with our University lawyers checking whether it would be safe to publish our paper.

As it happened, we got lucky this time, on two counts. First, the University agreed to indemnify those of us at Berkeley against any civil liability, if we were sued. Kudos for the administration! I can't say enough good things about their support for us. (Of course, the DMCA also comes with felony prohibitions on certain violations, and we were on our own in that respect (the University can't help with criminal liability), but civil liability was probably the more likely risk.)

Second, we talked with the engineers at Intel who designed HDCP, and they turned out to have very enlightened attitude about the whole mess. They thanked us for our work, and told us they would not sue us. If this had been any other company, though, things might have turned out differently.

Based on these two positive signs, we felt comfortable enough to publish, and our paper appeared in the ACM Workshop on Security and Privacy in Digital Rights Management 2001; URL below.
http://www.cs.berkeley.edu/~daw/papers/hdcp-drm01.ps

We were very fortunate. Nonetheless, it was not a good experience. I spent more time talking to lawyers then I did doing the actual research. We changed the way we wrote our paper, we changed the way we interacted with our researchers before our paper was published, and we wasted a lot of time on the legal aspects.

The DMCA is troubling. After spending many hours with lawyers examining the implications of the DMCA, I personally have stopped doing work on copyright protection systems, due to the legal overhead and uncertainties. (For instance, the "encryption research" exemption doesn't cover 1201(b) activity, along with all sorts of other oddities with which I'm sure you are very familiar.) I can't, in good faith, ask students I advise to take on such uncertain risks at this time. I consider this a perhaps cautious, but not irrational, response to the DMCA.

Yes, you may mention my name and all details of the situation in the hearing. This is all public information. In fact, it was featured as the cover story in SIAM News (a regular news magazine for mathematicians).
http://www.siam.org/siamnews/01-02/dmca.pdf
Let me know if there's anything else I can do to help!

-- David

USACM Recommendation

The fundamentally flawed approach of section 1201 criminalizes multi-use technologies rather than penalizing infringing behavior. During the current rulemaking proceeding, we urge that a distinction be made between circumvention for the purpose of obtaining infringing access to a work and circumvention for the purpose of developing new techniques to protect computer systems and networks against attacks, negligence, malfeasance, and vandalism, or to advance the continued innovation of software and digital computing.

USACM recommends that the Librarian of Congress provide an exemption to section 1201 that permits access to computer programs and databases that are protected by access control mechanisms in order to recognize shortcomings in security systems, to defend patents and copyrights, to discover and fix dangerous bugs in code, or to conduct forms of desired educational activities.

Thank you for the opportunity to appear before you today. I look forward to answering the questions of the panel.