I am responding to your request for comments regarding the new "circumvention" prohibition found in the Digital Millenium Copyright Act. I understand you will be deciding what classes of copyright works should be exempt from this particular provision.

I would ask you to interpret this prohibition narrowly, and to exclude large classes of copyrighted works from the prohibition. I speak as an academic researcher with considerable experience in the science of computer and telecommunications security and cryptography. I am very concerned that this prohibition will dramatically chill research into these general scientific fields as well as information of specific and immediate interest to society as a whole (e.g., evaluations of the security of everything from cellphones and DVD players to Web browsers and Internet security). I don't think that would be a desirable outcome.

Among other things, Section 1201 prohibits "reverse engineering" of any system that "effectively" controls access to a copyrighted work. We are beginning to see in the recent so-called "DVD cases" that some copyright holders are prepared to ask courts to interpret this provision very broadly, even when such interpretation may inhibit scientific research into computer security in general and into the security of specific systems.

Note that "reverse engineering" is crucial to determining whether or not a claimed-secure protection system is in fact secure. Thus, we risk ending up in a potential chicken-and-egg scenario: scientists and others are apparently prohibited from "reverse engineering" and otherwise circumventing effective systems, but this "reverse engineering" and circumvention step is exactly what is needed to determine whether the system is effective or not in the first place! One unintended consequence of this will be to chill research and study not only of effective systems, but of all systems.

In previous work, I have uncovered significant security holes in such every-day systems as digital cellphones and Web browsers. (See below for details.) I think these discoveries have important value for our society; for example, several of them were widely published in leading newspapers, sometimes on the front pages. But a broad reading of the DMCA "circumvention" prohibition would likely make this type of research illegal, and society would lose the opportunity to benefit from this sort of science.

Let me expand on this point a bit. I would like to point out two important aspects of my experience in this field. First, the devices I have studied would likely fall under section 1201, if the Copyright Office does not take steps to ensure that they are exempted. (For example, the encryption in digital cellphones effectively controls access to phone conversations, alphanumeric pager messages, and other data. Much of this speech, text, and data is likely to be subject to copyright protection. Thus, breaking the encryption of a cellphone may well count as circumvention of a device falling under 1201, unless the Copyright Office takes steps to ensure otherwise.) Second, even though this type of scientific work is otherwise legal and does not involve actually infringing the copyright of any copyrighted work, these scientific discoveries would not have been possible without actually engaging in circumvention and other activities covered by 1201. "Reverse engineering" is a crucial scientific tool in this field; and moreover, even if it were possible to study the system by some other manner without engaging in "reverse engineering" and other circumvention, it would nonetheless remain true that if one finds a defect it is still vital to verify the hypothesized flaw by trying it out, and that act of verification would count as circumvention under the definition of the DMCA.

The problem is that the DMCA does not make a distinction between (1) circumvention of a device that may process copyrighted data and (2) engaging in infringing use of a copyrighted work. Research on computer security often requires (non-infringing!) circumvention of access control mechanisms. Furthermore, the DMCA does not provide adequate protections to ensure that research and other studies will not be affected by the provisions of the DMCA. (I am aware of the section providing a partial defense for "encryption research", but it is becoming clear that they are wholly inadequate to achieve their stated goal. See, for instance, the recent "DVD cases".)

I would ask you to take notice of the recent "DVD cases", where intellectual property holders are attempting to silence not only programmers but also a scientist's academic evaluation of fatal flaws in the DVD security system. Please take special note of the early judicial findings that Section 1201 may ban all circumvention, even where users would otherwise enjoy fair use rights, even where there is no copyright infringment, indeed, even where there is no copyrighted work in sight.

I consider it likely that many researchers and consumers may be adversely affected in our ability to make noninfringing use of large classes of copyrighted works if they are not exempted from Section 1201.

I ask the Copyright Office to apply the following test: if non-infringing circumvention would be otherwise banned by Section 1201 for a class of works, please exempt those class of works from control under the DMCA. If you are unwilling to apply that test, I would then ask you to apply a slightly less aggressive test: if scientific research or other study of a class of works protected by some DMCA-covered device might involve or would require the non-infringing circumvention of that device, please exempt that class of works from the DMCA. Since advance designation and enumeration of all such classes of works may be infeasible and would certainly become outdated before the end of the relevant 3-year period, I would ask the Copyright Office to simply rule that all such classes of works should be considered exempted from the DMCA even if those classes have not been previously enumerated or explicitly listed by the Copyright Office.

I would also like the opportunity to give more background on the study of cryptography and computer security, on the importance of "reverse engineering" and circumvention, and related topics. This background information is a bit lengthy, so I have appended it after my signature.

But first let me thank you for the opportunity to comment on this proposed rulemaking, and I hope you will take my comments into full consideration. Please feel do not hesitate to contact me if you have any comments or questions whatsoever.

Signed,

David Wagner
University of California, Berkeley (for identification purposes only)

Address: David Wagner, Soda Hall, UC Berkeley, Berkeley, CA 94720-1776
Phone: 510 643 9435
Email: daw@cs.berkeley.edu

My work, my studies, and my teaching have given me extensive experience in the analysis of real-world security systems. The systems I have personally examined include supposedly secure systems used by hundreds of millions of people. Many of my discoveries have resulted not only in academic publications, but also in widespread news coverage in leading newspapers, magazines, and TV news shows. For example, in September 1995, a colleague and I reported serious security flaws in the techniques used for encrypting credit card numbers in the leading products facilitating the implementation of electronic commerce over the Internet. This discovery was reported on the front page of the New York Times, the front page of the business section of the Washington Post, and elsewhere.

In March 1997, two colleagues and I reported on the flaws in the privacy codes used by U.S. digital cellular phones, phones used by tens of millions of U.S. citizens. This work not only received widespread news coverage (e.g., the front page of the New York Times), but also helped convince the U.S. cellular standard committee to undertake a sweeping re-design of their security architecture.

In April 1998, two colleagues and I reported on the weaknesses in the privacy and billing-security protections found in GSM digital cellular phones. GSM is the European cellular telephony standard, with over two hundred million users worldwide. Again, this work received widespread coverage in leading newspapers such as the front page of the business section of the New York Times, page A3 of the Wall Street Journal, and other similar locations.

Publication of these types of flaws in supposedly secure systems serves a vital public interest. As our society becomes increasingly dependent on computers, telecommunications, and other information systems, it is important that our critical shared infrastructure be trustworthy and free of systemic security flaws. At the same time, as electronic commerce becomes more prevalent, criminals gain an increasing financial incentive to exploit security vulnerabilities in our critical systems. The vulnerabilities I described above clearly illustrate that the risks are very real: much of our existing infrastructure contains serious security vulnerabilities in its design and implementation, even though this fact may not have been apparent to the public.

History is replete with examples of governments, monarchies, and institutions placing confidence in supposedly secure systems and unbreakable code. For example, in World War II, through an enormous wartime effort the British and Polish succeeded in breaking a high-level German code called the Enigma and managed to keep this fact secret from the Germans and others for many years. I have read historians' accounts which suggest that this success may have shortened the war by as much as a year. The lesson of the Enigma is that we must be prepared for the adversary to expend unexpectedly large resources to break our security systems, and we must be ever-vigilant for the possibility that our most-trusted codes could have been broken without our knowledge.

Cryptography is one of the primary means of securing our critical information infrastructure against attack, and the study of cryptography must, I believe, form an essential foundation for our future information infrastructure. I believe that it is the scientific community's duty to study these issues and to report on systemic risks that the public at large may not be aware of. One must understand the risks in order to prevent them from recurring.

Outside security evaluation by independent third-party auditors forms a vital tool for ensuring the security of our critical information infrastructure. Third-party evaluations are critical because manufacturers do not always have the incentive or talent to undertake thorough examinations themselves. Researchers in the academic community often serve in this role, since they have no financial interest in the outcome of these evaluations. Other individuals and institutions participate as well. Think of the collective results of this work as a "Consumer Reports" for high tech mission-critical security systems.

Publication and circulation of results is the accepted way to share ideas and advance scientific knowledge about cryptography. It is widely held that the only way to learn how to build secure systems is to be intimately aware of the techniques a typical attacker might use: to be a good codemaker, one must be an accomplished code breaker. Moreover, it is not enough merely to study the theory of code-breaking: it is crucial to understand how real-world security measures are broken in practice, if we wish to build and deploy real security systems.

The combined knowledge of the cryptography research community is defined by published results, and extending the body of knowledge on how real-world systems get broken in practice is crucial to securing the systems of the future. Those who do not know history are condemned to repeat it; and publication forms the backbone of the academic community's history books.

The research projects I mentioned above have given me extensive experience in reverse engineering and the process of mathematically analyzing proprietary security systems.

Many security systems are distributed to the mass market implemented as a set of instructions for a computer to follow, specified in a low-level language designed to be convenient for a computer to process, but not necessarily especially convenient for humans to understand. The contents of these instructions to the computer are readily available to anyone who cares to look, but their meaning will not be readily apparent to anyone untrained in the field.

Reverse engineering in the field of computer system security is the art of understanding the meaning of the computer instructions and then presenting them in a simplified form so they may be more easily understood by other humans. Thus, the reverse engineer may be viewed as a linguist, a translator for an obscure machine-oriented dialect. In other words, reverse engineering consists of nothing more than studying a product in depth and summarizing its relevant features in a more comprehensible form.

Reverse engineering is often tedious, time-consuming, or simply boring, because computer programs are extremely verbose (by human standards), but it is not in principle difficult. Reverse engineering of supposedly secure systems can be performed by any trained individual anywhere in the world; this work is not restricted to graduate students and Ph.D. candidates. Individuals who lack high academic credentials have published some very important results.

Academic researchers do not always have time to undertake this type of reverse engineering effort. Instead, they rely on others to reverse engineer the product and make its inner working available in a form readily amenable to deeper mathematical analysis.

One of the reasons I have been so successful at analyzing real-world security systems is that I have worked closely with people who are very talented at reverse engineering.

It is a widely held view in the computer security field that it is unwise to deploy security mechanisms where reverse engineering the system allows one to evade its security measures. From a security point of view, attempting to keep the inner workings of your security system secret is ultimately futile and serves little purpose.

A broad interpretation of Section 1201 of the DMCA might encourage device manufacturers to employ very weak security mechanisms. For example, software manufacturers might be tempted to distribute their works in a slightly scrambled or obscured form -- not because this provides any real security, but rather because it is sufficient to argue that by merely attempt to build even the most minimally-secure, unsophisticated, insecure access control mechanism, they have triggered the provisions of the DMCA. This would be a very undesirable result, because it would encourage cyber-crime and other harms: many hackers -- especially those operating outside the reach of US law, in other countries and elsewhere -- will not be deterred by the DMCA. The risk is that hackers will have an easy time breaking into our legally-protected systems, and will wreak havoc on our critical infrastructure. This is not a good thing.

Note also that when security systems are distributed in a low-level computer language, before a third party can evaluate the security properties of the system one must make the operation of the system available in an understandable form. Consequently, reverse engineering is a common part of any independent third-party evaluation of the manufacturer's security claims. I am concerned that, if the Copyright Office does not take steps to ensure that "Consumer Reports" style third-party evaluation is exempted from the provisions of the DMCA, these independent evaluations will no longer be available to the public, despite the fact that these evaluations do not involve any infringement whatsoever.