Encryption Research Study

From: Jon Callas <jon@callas.org>
To: <dmca@ntia.doc.gov>; <crypto@loc.gov>
Cc: Jon Callas <jon@callas.org>
Sent: Monday, July 26, 1999 4:51 PM
Subject: Comments on sec. 1201(g) of the Digital Millennium Copyright Act

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

National Telecommunications and Information Administration
US Department of Commerce
US Copyright Office, Library of Congress

Dear Sir or Madam:

I am writing in response to your request for comments on section 1201(g) of the Digital Millennium Copyright Act.

I am a cryptographer and cryptographic engineer working in the industry on the design of cryptographic systems, including systems for information privacy and protecting intellectual property. I testified to Congress during the hearings on the DMCA on behalf of the industry. Consequently, I feel both qualified and obligated to respond to this RFC, as I participated in the creation of the DMCA.

The DMCA affects cryptographic research in a number of ways.

The DMCA directly affects cryptographic research because it makes "circumvention" an offense that is independent of infringement. It is my belief that the best thing that could be done to aid cryptographic research is to tie the circumvention to infringement, making it a form of aggravated infringement, similar to the way that other crimes can be aggravated by circumstance. I don't know of a single colleague of mine who would object to circumvention and infringement being a more serious crime than infringement alone. No one does real research that involves infringement. Changing this in the DMCA helps cryptographic research most. I must also point out other sections surrounding 1201(g) could also be removed; there would be no need for sections 1201(d), 1201(e), 1201(f), 1201(h), 1201(i), or 1201(j). All of these sections cover exemptions to circumvention that would not be needed if circumvention were an aggravation, not a separate offense.

In 1201(g), there are a few concerns about the exemption given that we have. They are in sections 1201(g)(2)(C) (obtaining permission), 1201(g)(3)(A) and (C) (disseminating information and notifying the work owner), and 1201(g)(3)(B) (whether someone is a legitimate researcher).

During the time the DMCA was being written, the main concern that the copyright-holders had would be that some infringer -- particularly a large-scale one -- would use "research" as an excuse when caught. While we can understand these fears, these remedies are not likely to work, they're more likely to stifle research.

An interesting aspect of today's research is that relative unknowns do some of the most important new work. The smart card vulnerabilities I described above were the first published research of some of the people who worked on it. Beyond that, some of the finest research today comes from groups of researchers who give themselves absurd or outlawish names such as "l0pht" (pronounced "loft") or "The Cult of the Dead Cow." These researchers are typically young, brash, have chips on their shoulders, are contemptuous of the authorities that created these security systems (often that contempt is well-placed), and have pop-culture attitudes that one typically associates with a rock-and-roll band. Perhaps most interestingly, they have an ironic attitude. Unlike published announcements from university or industry researchers which try to explain how smart the researchers are, these independent groups publish their results with a tone that emphasizes how stupid the researchers who created the broken system are. Make no mistake about it though, these young people with black t-shirts who like to call themselves "hackers" are nonetheless their generation's best and brightest when it comes to security research. This is relevant to 1201(g)(3)(B) because cryptographers often earn their stripes on their own, not under the tutelage of industry or universities. The problem with 1201(g)(3)(B) is that it is essentially a law against self-study. I know there are bad people in the world, people who infringe and threaten the copyright-holders, but this doesn't help the problem. It merely brings up new questions. What is a legitimate course of study? I believe that the real proof is whether or not they are infringing. If they're not infringing, this shouldn't be a problem. The true problem arises because circumvention is not tied to infringement.

The other sections are all parts of a common concern that is related to the above. They are part of an attempt to identify what legitimate research is, as opposed to a pirate mill. Again, they don't want to walk into a warehouse filled full of pirated movies (for example) and hear the excuse, "But I was only doing research." It's my opinion that this goes back to the tie between infringement and circumvention. The problem here is the warehouse full of pirated movies. The circumvention merely aggravates that offense.

These three sections I am concerned with cover obtaining permission, notifying the copyright-owner, and publishing the results. All of these sections are incredibly vague, for one thing. What constitutes a "good faith effort to obtain authorization"? And what if my good fail effort ends up with the copyright holder saying, "no"? (Which I will add, they would be daft to do otherwise! Who in their right mind would say, "I give you permission to hack me"?) I do note that the section does not require the researcher to obtain permission, merely to make a good faith effort to get it. But if you know that the answer to a question is going to be no, why bother asking?

Similarly, what is one to do after obtaining results? Who do you tell? What happens after you have told them, particularly if they have told you they don't want you to do research? It sounds to me like it's an invitation to be sued or charged with a crime. This is all very vague, and simply seems designed to stifle research.

The last section I question is disseminating information. What is an appropriate way to do it? Is it appropriate to publish in a scholarly journal? If so, what is a scholarly journals are acceptable, and which are not? What if they find it interesting, not so interesting that they want to publish it? Is a non-refereed journal acceptable? How about the front page of the New York Times? What about on my own web site? Unfortunately, 1201(g)(3) gives no guidance. It's impossibly vague.

Let me give an interesting real-world instance that happened earlier this year.

A movie studio (interestingly, one intimately involved in producing the DMCA) hired a colleague of mine to test a form of cryptographic protection that a vendor wanted to sell to them. My colleague found flaws in the system, and the movie studio declined to use it. I do not know if the studio asked permission to test it, or informed the vendor of their results, but should they have had to? I don't believe they should have to. (Mind you, it is certainly courteous to ask permission, and courteous to inform the provider. But I don't think it is wise to legislate courtesy.) Consumers Union doesn't have to ask permission to test a product. Nor do other organizations that test products. A customer does not have to ask a vendor to verify their claims. The DMCA should not be a law that protects snake-oil salesmen.

Unfortunately, those sections of 1201(g) are something that a creator of protection mechanisms that don't work can use as a club to silence those who would test it. They are also something that a legitimate researcher should not have to go through. These sections of 1201(g) do nothing more than hamper research, through their unreasonable requirements and vagueness. I see two ways to fix this problem, to strike them, or to tie circumvention with infringement.

Thank you for the opportunity to contribute.

/s/ Jonathan D. Callas
jon@callas.org

-----BEGIN PGP SIGNATURE-----
Version: PGP 6.0.2

iQA/AwUBN5zKG7E3nVmTg94GEQKgHgCfaHmVy4Uspotc73xEpQsKVLyXSLAAoM1J
gz6XDKVcshgvT+1HiQqkGxf5
=MyZk
-----END PGP SIGNATURE-----