Encryption Research Study

From: David Wagner <daw@cs.berkeley.edu>
To: <dmca@ntia.doc.gv>; <crypto@loc.gov>; <dmca@ntia.doc.gov>
Sent: Thursday, May 27, 1999 2:12 PM
Subject: Comments on 1201(g)

You asked for comments on the effect of section 1201(g) of the Digital Millenium Copyright Act. I think it will be harmful both to encryption researchers and to copyright holders.

Since 1201(g) doesn't take effect until October 2000, it is very difficult to talk about harm to encryption research that has already accrued. Therefore, I will focus on what evidence I can provide about the harm that is likely to result when the law takes effect.

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. For example, I personally know of one prominent encryption researcher (a colleague of mine) who has vowed to leave the United States before the law takes effect. I certainly do not expect a mass exodus, but due to the small size of the US encryption research community, the loss of even one good researcher is significant if the US is to establish a lead in digital copyright protection technology.

What is most disappointing is that 1201(g) will not help copyright owners -- it is a paper tiger, all bark and no bite. I would feel better about this loss to the research community if I felt there were some overriding benefit to be had from it, but I can foresee none. No copyright violator I have talked to is worried by 1201(g), and so I have to ask: does 1201(g) strike fear only in the hearts of legitimate encryption researchers?

To the extent that 1201(g) chills research into copyright protection schemes, it will inhibit progress in building workable rights protection schemes, and thereby potentially have a net negative effect on the security of copyright in the digital age. This would be an ironic but not entirely unexpected result.

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 noone, 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. I already have to worry about this threat, but 1201(g) makes the threat much worse: it places some of the burden of proof on me to demonstrate that I was proceeding in "good faith" (whatever that means), etc. In the past I have announced a number of serious flaws in widely-fielded

systems, and I think that my announcements have (on the whole) benefited our society; however, I have serious doubts about whether those previous announcements would pass muster under 1201(g)'s standards.

If other researchers share my concerns (and I think many do), this could have a detrimental effect on progress in copyright protection systems.

You asked for comments on the adequacy and effectiveness of technological measures for protecting copyrighted digital works. I can say that the current state of the art, on the whole, provides very weak protection for digital works. See e.g. research by Ross Anderson's group at Cambridge: they have demonstrated massive vulnerabilities in nearly all the commercially available tools for "digital watermarking" to protect copyrighted digital works.

Today, security for copyrighted digital works is poor. The situation is unlikely to get much better if 1201(g) chills research in this field.

Another effect of 1201(g) is that it will diminish the flow of information from non-academic amateur researchers, hackers, and "underground hobbyists". I have found that those people have made substantial contributions to cryptography; for me, as an academic, some of the amateurs I know have been a vital resource that were crucial to some of my academic discoveries. It is troubling to me that 1201(g)(3) considers well-intentioned hobbyists and amateurs to be presumptively suspect, purely because of their professions. I worry that they will be less willing to share their knowledge with me, for fear of prosecution. I feel that this is both unfair and detrimental to progress in the study of encryption.

To give a specific example, the "bugtraq" mailing list (on the Internet) is _the_ foremost, first-tier resource for learning about new security vulnerabilities as they are discovered. On "bugtraq", people who have discovered security vulnerabilities share them with the world so others can protect their systems; most often, the discoverers are not academic researchers, but rather come from the general public, and thus would not be able to rely on the protections in 1201(g)(3)(A), (B), and (C).

"bugtraq" is a vital information source for those who want to keep their systems secure. Will 1201(g) reduce the free sharing that makes "bugtraq" work, and thereby diminish the effectiveness of this resource? It might.

In summary, the law is poorly drafted and poorly considered; it will have ill effects both for us encryption researchers as well as for those who wish to have their copyrights protected; and I can only predict that the impact will be an unmitigated negative.

I urge you to let Congress know that 1201(g) should be reconsidered.