Testimony of Edward W. Felten
Associate Professor of Computer Science at Princeton University

Submitted to:

U.S. House of Representatives, Committee on the Judiciary
Subcommittee on Courts, the Internet, and Intellectual Property
Oversight Hearing on "Piracy of Intellectual Property on Peer-to-Peer Networks"
September 26, 2002

To the Distinguished Members of the Subcommittee on Courts, the Internet, and Intellectual Property:

I am writing to provide an independent perspective on some technical issues raised by Congressman Berman's proposed "P2P Piracy Prevention Act" (the "Berman Bill"). I offer this testimony in the hope that it will help the Subcommittee better understand the technical effects of the Berman Bill.

I write as an expert on computer security. I am an Associate Professor of Computer Science at Princeton University, and Director of Princeton's Secure Internet Programming Laboratory. I have published more than fifty research papers and two books, and my research has been covered widely in the national press. In addition to my service on corporate advisory boards, I serve on the Information Science and Technology (ISAT) advisory board of the Defense Advanced Research Projects Agency. I am co-chair of an ISAT study on "Reconciling Security with Privacy," and am a member of the National Research Council's study group on "Fundamentals of Computer Science." I have also served as the primary computer science expert witness for the Department of Justice (DOJ) in the Microsoft antitrust case, and as a technical advisor to the DOJ's Antitrust Division under both the Clinton and Bush administrations.

I share the Subcommittee's condemnation of widespread on-line copyright infringement. I support both legal action against copyright infringers, and technical self-help by copyright owners within the bounds of current law. The issue is not whether copyrights should be honored, nor whether the Berman Bill is well-intentioned, but rather what effect the bill would have.

I would like to bring two things to the Subcommittee's attention.

First, the Berman Bill's definition of "peer-to-peer" may be problematic. Peer-to-peer networking is not a new phenomenon, but has been the dominant mode of operation since the very beginning of the Internet. The World Wide Web itself is a peer-to-peer file sharing system, as the term "peer-to-peer" is commonly understood. More to the point, the Web clearly meets the Berman Bill's definition of "publicly accessible peer-to-peer file trading network." Therefore, *the bill, as written, flatly authorizes "self-help" attacks on the World Wide Web, and not just on users of file-trading networks like KaZaa and Gnutella.*

It seems difficult to redraft the bill to carve out the Web and other legitimate network services, without creating an escape hatch for the types of peer-to-peer networks that the bill's supporters would like to see covered. The reason for this difficulty is simple: there is really little difference at a technical level between the Web and peer-to-peer systems like KaZaa and Gnutella. The difference between these systems is not so much in how they are designed, but rather in what their users do with them.

(I also note in passing that the bill's exception for systems that "route all … inquiries or searches through a designated, central computer" may not have the effect that the bill's drafters envisioned. Nowadays large sites do not use a single "designated, central computer," but instead use a group of computers which cooperate to serve users' requests. It would appear, therefore, that the bill's "designated, central computer" exception would cover few if any of the large central sites for which the exception appears to be intended.)

Second, there is reason to doubt the efficacy of the technical measures that copyright owners want to use.

The copyright owners' representatives who testified in person at the Subcommittee's hearing could identify only one technical measure they plan to employ if the Berman Bill is enacted. This measure, which they call "Interdiction," was described in the written and oral testimony of Mr. Randy Saaf. Based on Mr. Saaf's description, "Interdiction" is apparently just a new name for a well-known type of denial of service attack[1].

A "denial of service attack" is a hostile action that exhausts the resources of a system or program, so that that system or program cannot operate, or can operate only in a degraded fashion. Some denial of service attacks seek to overwhelm a target computer's Internet connection with traffic, while others seeks to exhaust some other resource that the target needs.

For example, the so-called "SYN flood" denial of service attacks that (temporarily) disabled CNN, eBay, Yahoo!, and Amazon, in February 2000, disabled the target systems by initiating network connections with the targets in such a way that the targets were no longer able to accept further connections. Though the targets had plenty of spare communication bandwidth available, that bandwidth did them no good since they could not accept any more incoming network connections.

"Interdiction" operates on a similar principle. According to Mr. Saaf's written testimony:

> MediaDefender's computers hook up to the person using the P2P protocol being targeted and download the pirated file at a throttled down speed. MediaDefender's computers just try to sit on the other computers' uploading connections as long as

[1] For example, a speaker at this year's H2K2 "Hackers on Planet Earth" conference reportedly suggested using the attack that Mr. Saaf calls "Interdiction" against governmental and institutional Internet sites as a form of "online demonstration."

> possible, using as little bandwidth as possible to prevent others from downloading the pirated content....
>
> The goal is not to absorb all of that user's bandwidth but block connections to potential downloaders. If the P2P program allows ten connections and MediaDefender fills nine, we are blocking 90% of illegal uploading.

At present, Interdiction attacks apparently deny service only to the peer-to-peer program running on a user's computer, and not to any other programs. The designers of peer-to-peer software will not simply accept this situation, but will respond by modifying their software to thwart such targeted denial of service attacks. They might do this, for example, by eliminating the self-imposed limit on the number of connections the peer-to-peer program will accept. These countermeasures will start an "arms race" between copyright owners and peer-to-peer system designers, with copyright owners devising new types of targeted denial of service attacks, and peer-to-peer designers revising their software to dodge these targeted attacks.

Computer security analysis can often predict the result of such technical arms races. For example, analysis of the arms race between virus writers and antivirus companies leads to the prediction that antivirus products will be able to cope almost perfectly with known virus strains but will be largely helpless against novel viruses. This is indeed what we observe.

A similar analysis can be applied to the arms race, under the Berman Bill's rules, between peer-to-peer authors and copyright owners. In my view, the peer-to-peer authors have a natural advantage in this arms race, and they will be able to stay a step ahead of the copyright owners[2]. Copyright owners will be forced either to give up on the strategy of narrowly targeted denial of service attacks, or to escalate to a more severe form of denial of service, such as one that crashes the target computer or jams completely its Internet connection. I understand that these more severe attacks are currently illegal, and would not be legalized by the Berman Bill, so such an escalation would not be possible within the law even if the Berman Bill is enacted. I conclude that the Berman Bill as written is unlikely to do copyright holders much good in the end.

Contact information:

Edward W. Felten
Dept. of Computer Science
Princeton University
35 Olden Street
Princeton, NJ 08544

(609) 258-5906 (voice)

---

[2] [2] I understand that the House of Representatives uses technical means to prevent peer-to-peer file trading by its employees. Of course, the ability of an organization such as the House to control the use of *its own* systems does not imply that copyright owners can exert the same level of control on *others'* systems.

(609) 258-1771 (fax)
felten@cs.princeton.edu