## **Congress Unknowingly Undermines Cyber-Security**

## Jonathan Band<sup>1</sup>

Since 9/11, much public attention has focused on the tradeoff between security on the one hand and civil liberties and privacy on the other. We see this conflict every day when we read about the detainment of foreign nationals or the latest homeland security initiative such as the Pentagon's Total Information Awareness program. We personally experience it when we are searched before we board an airplane.

There is, however, another post-9/11 policy conflict that has received far less public attention. This is the growing conflict between cybersecurity and intellectual property.

For several years the entertainment industry had argued that the Internet in general and peer-to-peer networks in particular enable intellectual property infringement on an unprecedented scale. Industry representatives claim that this infringement cuts their profits and diminishes their incentive to invest in new products.

Accordingly, the entertainment industry has lobbied Congress to adopt a variety of measures aimed at facilitating the enforcement of intellectual property rights. Unfortunately, these measures have the unintended consequence of undermining cybersecurity.

For example, in 1998 Congress passed the Digital Millennium Copyright Act. One provision of the DMCA prohibits the circumvention of technological measures that protect access to copyrighted works. The provision's intent was to impose legal penalties on hackers who penetrated the encryption and other technological measures copyright owners would use to protect their works in the digital environment.

As the DMCA was working its way through Congress, technologists pointed out that the bill as drafted could outlaw the research and testing necessary to develop new cybersecurity products. In response, Congress included in the DMCA two narrow exceptions for encryption research and security testing.

In the four years since the DMCA's enactment, it has become increasingly clear that these exceptions are simply too narrow. Computer science professors have found themselves entangled in litigation because of their academic activities, and universities and software companies have had to include attorneys in the research and development process to ensure compliance with the DMCA's arcane terms.

In this way, the DMCA has hindered the development of technologies that can protect computer networks from cyberattacks. Indeed, Richard Clarke, the head of the

<sup>&</sup>lt;sup>1</sup> Jonathan Band is partner in the Washington, D.C. office of Morrison & Foerster LLP and an adjunct professor at the Georgetown University Law Center.

White House office of cyberspace security, recently called for the amendment of the DMCA because of its "chilling effect on vulnerability research."

This year, the entertainment industry supported another legislative proposal that would have had an even greater negative impact on cybersecurity than the DMCA. The P2P Piracy Prevention Act of 2002 would have permitted copyright owners to launch denial of service (DoS) attacks on computer users who "shared" copyrighted works over P2P networks. Until now, Internet service providers have assumed that all DoS attacks are unlawful and require an immediate response. The P2P bill would completely undermine this approach. Before responding to a DoS attack, a service provider would have to determine its legitimacy. This, of course, would delay the service provider's response to serious illegitimate attacks.

In the next Congress, the conflict between intellectual property rights and cybersecurity will come into greater focus. The P2P bill probably will be reintroduced. At the same time, a bill amending the DMCA to exempt security research activities from legal liability will also be introduced. These two bills heading in opposite directions will force Congress to confront this issue head-on.

Unlike the conflict between security and privacy, the conflict between cybersecurity and intellectual property is completely avoidable. Copyright owners have numerous means at their disposal for protecting their intellectual property without compromising cybersecurity. These include litigation, spoofing, and the development of new business models that discourage infringement. Moreover, copyright owners could promote the development of stronger technological protection measures, which could actually enhance security. These means might be more expensive than those permitted under the DMCA or the P2P bill, but the cost to society of cyberattacks that cripple our critical information infrastructure will be far greater.