A BRIEF ANALYSIS OF THE "SUPER DMCA" (THE DRAFT MODEL COMMUNICATIONS SECURITY ACT)

Background

Over the past two years, lobbyists from the Motion Picture Association of America (MPAA) have been lobbying in state legislatures for passage of a model "Communications Security Act." This act, which has already been passed by six states – Delaware, Illinois, Maryland, Michigan, Pennsylvania and Wyoming – has been represented to legislatures as little more than an updating and minor amendment of existing state laws designed to prevent theft of cable or telephone service.

A close reading both of the acts that have been passed and of the "draft model act" shows, however, that the proposed law could have a far broader impact – it could undermine existing consumer rights to use cable, telephone and Internet services, and could also hurt technological innovation and the development of new products that benefit consumers.

The model act, together with the state acts that already have been passed or that currently are being proposed, are often referred to by some opponents as "super DMCAs" or "state DMCAs" – in reality, their scope is different from, and far broader than, the federal Digital Millennium Copyright Act.

Overbroad Definitions

The acts protect "communication services," which include any "service lawfully provided for a charge or compensation" delivered via electronic means using virtually any technology. This includes every wire in your house for which you pay a fee, including your telephone, cable TV, satellite and Internet lines. This category also sweeps in any Internet-based subscription services for delivery of copyrighted materials, including digital music services such as pressplay, MusicNow, or Rhapsody.

The acts would regulate the possession, development and use of "communication devices" and "unlawful access devices." A "communication device" is virtually any electronic device you might connect to any communication service. The definition of "unlawful communication device" is somewhat narrower, sweeping in any device that is "primarily designed, developed, …possessed, used or offered… for the purpose of defeating or circumventing" a technological protection measure used to protect a communication services.

What the Acts Prohibit

The proposed bills generally prohibit four categories of activity:

(1) Possession, development, distribution or use of any "communication device" in connection with a communication service without the express authorization of the service provider.

(2) Concealing the origin or destination of any communication from the communication service provider.

(3) Possession, development, distribution or use of any "unlawful access device."

(4) Preparation or publication of any "plans or instructions" for making any device, having reason to know that such a device will be used to violate the other prohibitions.

1875 Connecticut Ave, NW
Suite 650
Washington, DC 20009

T 202.518.0020
F 202.986.2539
publicknowledge.org

The Proposed Acts Are Unnecessary

The MPAA has argued that this law is necessary to "update" existing state laws to prevent "Internet piracy" and "cable theft." But copyright infringement and cable-service theft are already expressly prohibited under current state and federal laws. In addition, any service provider who believes a subscriber has violated the terms of his or her service contract can terminate the contract.

The MPAA has not identified any specific problem that is not already addressed by existing law. Nor have state law-enforcement personnel called for or supported these proposals.

Controlling Consumers and Undermining Innovation

These prohibitions, together with the broad definitions, dramatically expand the power of entertainment companies, Internet service providers, cable companies and others to control what citizens can and can't connect to the services that they pay for. If enacted, they will slow innovation, impair competition and seriously undermine consumers' right to choose what technologies they use in their homes to lawfully access these services.

These acts could make a citizen a criminal for simply connecting a TV, PC, TiVo or VCR (all of which can "receive" communication services) to the cable TV line in his or her living room without the cable company's permission. It could also make a citizen a criminal for connecting a Wi-Fi wireless gateway (which can "retransmit" Internet traffic) to your DSL or cable modem line without the permission of your ISP.

The shift proposed by these bills is radical: ***all technology that is not expressly permitted becomes forbidden.*** This would give communication service providers unprecedented control over the home entertainment and the technology marketplace.

As noted above, the proposed bills also forbid a consumer from connecting anything to a communication service without the service provider's express authorization. This creates an enormous opportunity for anticompetitive conduct. Broadband Internet service providers, for example, could require that their subscribers use only a particular brand of PC or operating system. AOL could effectively ban its subscribers from using any instant messaging software other than its own. Cable-TV providers could limit subscribers to using only certain brands of VCRs and could ban TiVo in favor of their own proprietary PVR technologies. This flies in the face of the Federal Communications Commission's longstanding policy to encourage the development of open, interoperable standards for cable-compatible televisions, and to allow users to attach their own equipment to cable or telephone networks, so long as doing so does no harm to the network.

"Intent to Defraud" Is Not A Fix

In response to criticism, the MPAA has offered to modify the proposal by adding an "intent to defraud" requirement for liability. While that language may address some concerns, it does not adequately narrow the scope of the act, and in any case has been incorporated inconsistently or not at all in the various proposed or enacted state statutes. Furthermore, is unclear whether a civil breach of service contract terms would be interpreted to add up to a criminal "intent to defraud."

Attack on Privacy and Anonymity

The bills include a ban on devices that "conceal … the existence or place of origin or destination of any communication." On its face, this ban would outlaw many ordinary home-networking products, including routers that include "network address translation" and/or security firewalls, because they conceal some user activities and identifying information from the larger Internet. The use of "virtual private networking" (VPN) software by corporations to secure communication with off-site employees could also be swept up by this provision. Products like Anonymizer that are designed to protect the privacy of Internet users against advertisers like Doubleclick might also be implicated.

Broad and Bad Remedies

The proposal provides a number of provisions and remedies that add up to bad public policy. These include:

- Adding a civil remedy to broad criminal statutes, which enables private parties to exercise the same kind of discretion as a prosecutor, but without the same degree of public accountability.

- Enabling state courts to order "remote downgrades" of software or equipment by vendors on a nationwide basis through "auto-update" features.

- Imposing one-sided fee-shifting (losing defendants have to pay attorneys' fees for the winning plaintiff, but the converse is not true).

- Allowing automatic preliminary injunctions, without any showing of likely actual damage, irreparable harm or inadequate remedy at law.

- Awarding of statutory damages that may be crippling to defendants, even when a plaintiff cannot show any actual damages at all.

Time to Be Heard

Laws like the Super-DMCA make it clear that ***Hollywood has overlooked or disregarded vital consumer and public interests in eagerness to craft new (and superfluous) laws to "protect" its copyrighted works***. Public Knowledge believes it is legitimate for Hollywood to protect its copyright interests, but also believes it is bad policy to attempt to do so by making it ***illegal*** for citizens and consumers to do anything but what the studios and other corporate content providers dictate.

Public Knowledge is working to counter the efforts of the MPAA on these bills, but we cannot do it alone. We ask that you educate yourself on this issue, contact your local representative, and reassert your rights as a citizens and consumers.

For further information, contact Mike Godwin, Senior Technology Counsel, Public Knowledge at 202-518-0020 or godwin@publicknowledge.org