

Pending Florida legislation would take away your right to potentially own or operate a TiVo, network firewall, or Wi-Fi device. Not to mention your right to privacy, your right to invent and innovate network devices and software, and possibly your right to make a living.

Summary

At its heart, this proposed legislation is about the Motion Picture Association of America (MPAA). They're scared that expanding availability of broadband services will allow movies to be downloaded in a manner similar to how music files are already today, thus radically altering their future business model, as has happened to members of the Recording Industry Association of America (RIAA).

In response, the MPAA has been using the (Federal) Digital Millennium Copyright Act against Internet service providers (ISPs), warning them that failure to stop their customers from making copyrighted material available online puts them in violation of the law. While some respond by cracking down on file trading by their customers, others have told the MPAA that they can't always trace who is doing what. Customers using a router, encryption, network address translation (NAT), or firewall software can keep their computer uses private, they say, and out of ISP's control.

To solve the "problem" of customer privacy, the MPAA had a law firm draft a "model" for the legislation pending in Florida now: a direct attempt to bypass consumers' and users' rights at the state level — disguised as an attempt to expand cable theft laws.

In detail

The Florida bills, S1078 and H0079, are amendments and changes to Communication Services, s. 812.15 of the Florida Statutes. These changes weren't asked for by law enforcement for state prosecutors, they were lobbied for by a special interest: the MPAA. There are already innumerable laws on Florida's books outlawing hacking, theft, and fraud. These laws would add new, unnecessary provisions for ISPs nationwide to understand, new paperwork and lost time for Florida's businesses, and new requirements Florida's consumers will not comprehend.

The MPAA is sending an seemingly-straightforward public message with respect to the legislation they carefully crafted. Anyone who opposed the bills must be "against shoplifting laws that would punish someone from stealing a movie at Blockbuster," MPAA Vice President Vans Stevenson says. The measure is a test of "whether you subscribe to the moral compass this country was founded on." (*Washington Internet Daily*, Louis Trager, 4/9/03)

"The entertainment companies state that these laws need to be updated to combat digital piracy," says a letter from the Association of Research Libraries, the American Association of Law Libraries and the American Library Association. "While digital piracy is a serious problem, some of the proposed amendments will undermine the ability of libraries to provide important information services."

John Palfrey, executive direction at the Berkman Center for Internet and Society at Harvard Law School, testified to the committee considering a nearly-identical Massachusetts bill that computer scientists who published reports on weaknesses in telecom security systems could be prosecuted. “I’ve never heard anybody — not a prosecutor, not anybody in law enforcement — saying that we need these laws,” he said. “The only people I hear saying we need these laws are the Motion Picture Association.” (Boston.com (*The Boston Globe*), Hiawatha Bray, 4/15/03)

Palfrey goes on to testify, “We must also see this bill in its proper national context. This bill is a part of a concerted national special interest campaign. This bill has been proposed as a one-size-fits-all piece of legislation in numerous states around the country.” (This would include the Florida bills, which are based on the same “model” legislation from the MPAA.) “Who wants this bill?” he asks, and reminds the Massachusetts legislators — as we should remember here in Florida — that, “this bill was not written for this state and it should not be enacted in this state.”

David McClure, president of the U.S. Internet Industry Association, said that under the MPAA’s “model” legislation, “any technology [the MPAA] doesn’t like is banned. Not only is it banned, but it opens you to criminal penalties for its use. If you use a computer, you could be a criminal.” (News.com, Declan McCullagh, 3/28/03) The obvious comparison here is filtering software: these proposed laws would represent a change from a system that blocks only bad web sites (devices) to a system that only allows approved web sites (devices). Since filter software ineffectiveness is well proven — cited by the U.S. Supreme Court as a reason to strike down library censorship, for instance — why extend that model to devices connected to the network? Simple. The MPAA wants control. Proposed changes to the Florida Statutes are based on the same MPAA “model”.

Chris May, a Colorado ISP owner, wrote in response to laws proposed there that “50 percent of my customers use the sharing feature at home, since it allows each child to have his own computer and use it simultaneously. 100 percent of businesses, government offices, schools, and nonprofits use either NAT or share,” putting them in violation of that legislation, also based on the MPAA “model”, by using firewalls or other techniques to ensure privacy. His customers and countless others in states with legislation or proposed legislation like this could easily be guilty of “intent to defraud” by knowingly bypassing an ISP’s rules against Wi-Fi devices to share a single connection, for instance.

“This is stunning in its overbreadth; [it] would appear to make most computer security research illegal, since it would be illegal to even talk about how somebody might try to defeat a security measure. As a computer security researcher, I consider that a big problem. In this case, though, that problem is small potatoes compared to the greater harm . . . the bill would do,” Princeton Prof. Edward Felten wrote in his weblog, *Freedom to Tinker*. “Notable has been the silence of the law enforcement community. Why? Presumably because law enforcement already has the tools it needs to prosecute the bad guys.”

Perhaps most influential to government officials and the general public alike, however, is someone with their eye on the big picture: Alan Greenspan, Federal Reserve Chairman. On April 4, 2003, at the 2003 Financial Markets Conference, he said:

Market economies require a rule of law. A society without state protection of individual rights, especially the right to own property, would not build private long term assets, a key ingredient of a growing modern economy. Yet an excess of rules — in the extreme case, central planning — has also been shown to stifle innovation and produce economic stagnation.

In recent decades, for example, the fraction of the total output of our economy that is essentially conceptual rather than physical has been rising. This trend has, of necessity, shifted the emphasis in asset valuation from physical property to intellectual property and to the legal rights that inhere in the latter. Though the shift may appear glacial, its impact on legal and economic risk is only beginning to be felt.

Indeed, the nature of intellectual property is importantly different from physical property. In particular, one individual's use of an idea does not make that idea unavailable to others for their own, simultaneous use. Furthermore, new ideas almost invariably build on old ideas in ways that are difficult or impossible to delineate.

If our objective is to maximize economic growth, are we striking the right balance in our protection of intellectual property rights? Are the protections sufficiently broad to encourage innovation but not so broad as to shut down follow-on innovation? Are such protections so vague that they produce uncertainties that raise risk premiums and the cost of capital?

Like the now-famous "irrational over exuberance" speech, Chairman Greenspan is clearly indicating that overreaction can cause serious harm. His words, combined with the others mentioned above, demand defeat of this special-interest legislation.

How much could you be liable for?

I work full-time for an agency in the Tampa Bay area, ensuring network security and document privacy for clients' new and upcoming products. On a daily basis, my work for small and large Florida companies — use of encryption, firewalls, NAT, Wi-Fi access points — requires me to use techniques and technologies that would potentially be illegal under these new statutes.

Sarah Deutsch, associate general counsel for Verizon Communications (a ISP with service in Florida — including my home), says Verizon "could be liable if one of our customers did something that violated" the Massachusetts version of this legislation. Presumably, since the Florida bills are nearly identical, Verizon and other ISPs could be liable here, too. These ISPs could pass costs associated with these new laws to Florida consumers, including you and me. Further, the proposed legislation is so overbroad as to present lawyers with infinite opportunities to interpret and argue "intent," potentially costing thousands in lawyers' fees — fees that as a defendant you're not allowed to recover from the suing party under the MPAA "model" legislation, should you eventually prove your innocence. ("State 'Super-DMCA' Legislation", Electronic Frontier Foundation, April 14, 2003.)

And, as consumers, we would have to be wary of a whole new set of potential violations. How wary? A Michigan college student wrote a program that scanned, indexed and made available to his University's network all available shared files, *duplicating a function built in to Microsoft Windows XP*. Because these files included other students' copyrighted music files, the RIAA sued that student for \$97.8 billion dollars. (The Freep (*Detroit Free Press*), Heather Newman, 4/5/03. And that's not a typo — billion.) To date, the RIAA has not sued Microsoft.

Consider, for a moment, the following scenario: your business or home has a Wi-Fi access point, allowing several employees or family members to simultaneously use multiple computers on the Internet. Your ISP doesn't allow it, but doesn't do anything because they don't know about it — they respect your privacy once the circuit enters your business or home. However, the RIAA

or MPAA attempts to scan your network and can't, due to the firewall and encryption used in the Wi-Fi device, and notifies your ISP. Suddenly, because you've intentionally violated your service contract — “intent to defraud” — your business or home, your livelihood, is potentially on the hook for thousands or tens or hundreds of thousands of dollars of damages due to these proposed statutes. That's before the MPAA or other organizations move in, taking advantage of these laws, to “inspect” your computers for violations. Disruptive to your business is putting it mildly, especially if your business relies on its computers and an Internet connection to get essential business done; disruptive to your home is a joke in the face of devastating damage awards for desiring a convenience already available to Florida homes and businesses that your ISP doesn't happen to allow.

That scenario is not fantasy: it's what could happen to you, your home, or your business if these proposed statutes pass the Florida Legislature. Take the time to defend your rights: notify your Legislator that he or she must work to defeat these special-interest laws.

“Portal to democracy”

On April 16, 2003, CNet's News.com ran an article titled, “Software rams great firewall of China.” The United States government, through its citizens, is giving Chinese citizens the opportunity to do what the MPAA is specifically trying to outlaw here, in the various laws proposed and already enacted around the U.S.

“The idea behind the U.S.-backed software,” CNet writes, “is to allow someone trying to evade a firewall to tunnel under it via a third-party computer not blocked by the firewall. The software, which uses Secure Sockets Layer (SSL), lets the person who installs it set up a miniature Web site through which a firewall-restricted surfer can access the rest of the Web.

“In addition to circumventing firewalls, the software also creates anonymity by covering the Web surfer's tracks and leaving no record of what sites he or she visited beyond the miniature Web site.”

The article also quotes Ken Berman, program manager for Internet anticensorship at the International Broadcasting Bureau, which puts out the Voice of America and other programs: “We're trying to get people to run circumventor software. We like to call our program a portal to democracy.”

All of the activities mentioned in that article would be banned under this proposed legislation. If these changes are passed by the Legislature, offering a “portal to democracy”, which could also be potentially used to unknowingly share copyrighted materials — whether in the service of democracy or not — makes you a criminal.

Who are we, as Floridians, to argue with the U.S. Government's promotion of “portal[s] to democracy”? Who are we, to allow our rights to be swept away yet again by special interests? We should stand up to the MPAA and prevent the Florida Legislature from passing these laws taking away rights essential to doing business, allowing innovation, doing research, and protecting private information in Florida. Go to <http://taxonomy.myflorida.com/Taxonomy/Government/Legislative%20Branch> to contact your Legislator today.

By Giles Hoover, Bradenton, Florida, April 21, 2003

This work, *Portal to Democracy in Florida*, carries a Creative Commons Public Dedication, which means I place this document in the public domain. More details are available; see <http://creativecommons.org/licenses/publicdomain> for the specific licensing document.