INTERNET ARCHIVE
WaybackMachine

http://www.todaysengineer.org/2012/Feb/SOPA.asp

7 captures
28 Mar 2012 – 26 Mar 2014

About this capture

SOPA/PIPA Defeated... For Now

BY ERIC BURGER

There has been a lot of action, articles and discussion recently about legislation that proponents at one extreme offered would save hundreds of thousands of jobs and add between $50B and $250B to the U.S. economy per year, and detractors at the other extreme argued would turn the United States into a police state and terminate the first and fourth amendments to the Constitution. As with many things in life, the truth lies somewhere in between.

"Even with SOPA off the table, there are valid piracy issues, an ongoing need to reform copyright to align with real incentives for creators and finally future issues that touch the Internet which now has a community of

Intellectual property rights (IPR) and communications have had a long-standing love-hate relationship. Without communications technology, authors and publishers of IPR would have limited, if any distribution of their works. However, with digital technology and modern communications, IPR holders find that it has been getting progressively easier for people to make infringing distributions of protected content.

The infringing use of content encumbered with IPR (we will call this "IPR" for the rest of this article) is a real issue. While there is great debate as to the magnitude of the problem, just about everyone agrees there is a problem. For example, the software industry faced rampant piracy in the 1980s. The industry responded with mostly technological solutions. Some manufacturers built their own proprietary

short circuits

Engineering Hall of Fame: Pavel Nikolayevich Yablochkov

World Bytes: John Glenn, An American Hero

viewpoints

reader feedback

archives

career articles

policy articles

all articles

2012

Dec Nov Oct Sep
Aug Jul Jun May
Apr Mar Feb Jan

2011

Dec Nov Oct Sep
Aug Jul Jun May
Apr Mar Feb Jan

archive search

Search Now

hardware. If you wanted to run their software, you had to buy the hardware from the IPR holders. Later, with the widespread adoption of the personal computer (PC), software manufacturers required security hardware, in the form of boards inserted into the PC or dongles that attached to a port on the PC. However, there were costs to the IPR holders for manufacturing, distribution and support of the hardware. Moreover, the customers had even greater costs for installing and maintaining this hardware, as well as costs from compatibility issues. The software industry tried using characteristics of particular platforms, such as disk sectors that were not legal but readable and not normally writable to use the software media, first flexible disks and then CDs and DVDs, as the hardware key.

giants taking active interest."

— Jim Isaak, past president of the IEEE Computuer Society, as posted on his blog [read on]

Comments on this story may be sent directly to *Today's Engineer* or submitted through our online form.

Because of the complexities and costs associated with hardware-based copy protection, the industry has moved to cryptographic approaches. These approaches run the gamut from trivial passwords that can easily be defeated, scrambling of code that dynamically becomes plain text to make it virtually impossible to grab an unencrypted copy, to tying the copy to a specific element of the hardware platform, such as an Ethernet MAC address or CPU identifier. Floating licenses became popular in the late 1980s and 1990s for high-cost, but shared applications.

Another approach, from the 1970s, is to use pricing to drive behavior. For example, the price of Microsoft 4K BASIC on paper tape was not much more expensive than what it would cost to make a copy. Conversely, the license from AT&T for Unix™ was extremely expensive, but presumed the user would make internal distributions.

Finally, we have a number of audit models, from explicit visits or electronic audits for large enterprises through software packages that "phone home" when used. This enables the IPR holder to send polite notices to people infringing on the holder's IPR.

There have been a number of legislative approaches to address the problem of infringing use and distribution of IPR. In 1988, Congress passed the *Digital Millennium Copyright Act* (DMCA), which was an amendment to the *Copyright Act of 1976*. Congress (and the World Intellectual Property Organization) recognized that digital media is much easier to copy than print, analog audio, and analog video media. The DMCA made it unlawful to traffic in digital copies of IPR. The DMCA also made it unlawful to reverse engineer any technological solutions to copy restrictions. That is, it is unlawful to break copy protection. There are a number of important exclusions, such as for encryption research, for libraries and educational institutions for evaluation purposes, and there was a time limit for implementation if it was shown that these technological copy protection solutions impeded fair use.

What was critically important in the DMCA was that it explicitly stated that communication carriers are not responsible for user's transmissions. Moreover, service providers, such as Internet service providers and Web hosting providers, would not be responsible for holding infringing copies of IPR, so long as those copies came about due to the normal operation of the Internet, such as caching. User-originated content, such as a user posting a copyrighted video, is only an issue for the service provider if the owner of the IPR notifies the service provider the material has encumbrances. In this case, the service provider must take down the material, either by physically removing copies if the service provider is a hosting firm or removing links if the service is an indexing or search firm. In any event, if the service provider's business is to materially profit from the distribution of infringing IPR, the DMCA makes it clear they are violating the law.

The DMCA protects IPR holders by enabling them to require the removal of infringing copies of their IPR. It protects service providers by providing a deterministic process that allows platform providers to host user generated content. Finally, the DMCA protects users by requiring a court process for the take down provision. The DMCA also protects user rights by requiring a court order for the service provider to reveal who the user is who posted or retrieved the infringing content.

One limit of the DMCA is the Court can only send notices to U.S. service providers. There is no mechanism to send notices to foreign service providers. Even if there were a mechanism, there would have to be cooperation from the foreign governments to take down the infringing content. Addressing this issue of foreign service providers were two legislative initiatives, the *Stop Online Piracy Act* (SOPA) and the *Protect Intellectual Property Act* (PIPA). Their goal is to remove access to infringing content stored outside the U.S. by domestic users. Since the Court cannot take down foreign content, the approach was to create a distinct U.S. network, disconnecting the U.S. population from the open Internet. The idea of making parts of the Internet inaccessible was hard for most people to accept — especially given the Internet was invented in the United States — just to satisfy IPR holders. Moreover, the same technology used for such blocking is, from a technical perspective, identical to the technology used to censor speech. Lastly, the method proposed, domain name system (DNS) filtering, broke key Internet infrastructure. DNS filtering makes access to infringing content slightly more difficult than over the open Internet, but at the cost of potentially exposing U.S. citizens to organized crime. This occurs by circumventing the filtering mechanism by using untrusted DNS operators. Moreover, DNS filtering could potentially halt deployment of DNSSEC. DNSSEC is a critical Internet infrastructure technology that ensures that when you ask for a particular web site, like www.ieee.org, that you get the real IP address, not the address of, for example, the ITU-T with a phishing site to try to get you to log into what you think is the IEEE. DNS filtering is indistinguishable from a man-in-the-middle attack, and the design of DNSSEC indicates this attack to the user. Since users would get potentially lots of error messages, service providers would have to deal with lots of support calls. Since support calls are expensive, service providers would most likely turn off DNSSEC. This would subject U.S. citizens and businesses to cache poisoning, bank account theft, identity theft, theft of commercial information, and so on.

Besides DNS filtering, SOPA and PIPA proposed blocking financial transactions with targeted Web sites. In addition, they proposed allowing pretty much anyone to assert there were infringing activities at the Web site, which in practice would be sufficient to start the take down process. At the time of the writing of this article, SOPA and PIPA have been tabled. Now under consideration is a bill called the *OPEN Act*. OPEN takes the concept of shutting off financial transactions with infringing Web site and adds a set of proposals for due process. The *OPEN Act* imposes costs for frivolous notices and gives the service provider an opportunity to be heard. Otherwise, it follows the basic outline of the DMCA. There are some provisions that are controversial.

In fact, because of the controversies and the possible technical impacts of any legislation, the IEEE-USA Committee on Communications Policy and Intellectual Property Committee has formed a joint work group to address IPR and communications legislation. If you are interested in participating, please send a message to Erica Wissolik, e.wissolik@ieee.org

Comments on this story may be emailed directly to *Today's Engineer* or submitted through our online form.

Dr. Eric Burger is past chair of IEEE-USA's Committee on Communications Policy and chairs IEEE-USA's joint work group on IPR and communications legislation. Dr. Burger is research professor of computer science and director of the Georgetown Center for Secure Communications at Georgetown University in Washington, DC.

home

Copyright © 2012 IEEE