WebMemo
Published by The Heritage Foundation
No. 3459
January 17, 2012

Online Piracy and Internet Security: Congress Asks the Right Question but Offers the Wrong Answers

Paul Rosenzweig

The Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) are well-intentioned House and Senate proposals aimed at stopping the theft of intellectual property through foreign-based websites. Intellectual property is a critical and important form of property. The Framers understood that well enough to authorize the establishment of intellectual property protections when they drafted the Constitution, and we have had copyright protection in America ever since.

Some malicious actors use the Internet as a means of violating the copyright interests of creative producers in a wholesale manner. It is common to find free copies online (often of pretty good quality) of many recent movie and recording releases that can be downloaded and enjoyed without the original creators receiving compensation. That is fundamentally wrong, and the intent of the pending bills—to end online piracy—is the right idea.

But the manner in which these bills attempt to achieve their ends likely would not work. In fact, they would make the Internet generally less secure for everyone.

Understanding Internet Protocols. At the heart of the problem is the requirement that, as PIPA puts it, operators of the Internet can be ordered to "take... technically feasible and reasonable measures" to prevent domain names from resolving to their own Internet protocol addresses. The Internet Protocol or IP address is the number string that is the actual address of a website; the domain name is its common text name. Typically, a domain name resolver function translates, for example, a domain name like "heritage.org" into "93.184.221.133." What PIPA and SOPA say is that operators like Verizon could be ordered by a court to stop that translation function.

To understand why this is one of the significant problems raised by the bills requires a bit of a technical detour into the workings of the Internet. To begin with, the current protocols of the Internet do not have an "authentication" function. The Internet is designed to move information effectively and efficiently from one place to the next, but it does not have a general security system in place to warn people when their traffic is being hijacked.

Without that sort of security system, efforts to navigate the Web are susceptible to "man-in-the-middle" attacks where the malicious actor steps into the middle of a conversation and hijacks it by making independent connections with the victims.

This paper, in its entirety, can be found at:
http://report.heritage.org/wm3459

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

From the middle vantage point, he can relay messages between the victims, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the malicious actor.

The Internet is also susceptible to pure spoofing—for example, where your request to connect to your bank at "chase.com" is maliciously redirected to a phony "chase.com" website and your login information is collected. For many years, the engineers responsible for the specifications of Internet traffic (the Internet Engineering Task Force, or IETF) have been aware of this vulnerability—which costs millions of dollars every year in theft—and they have been working on a solution.

Internet Security Measures Already Proposed. That quest has resulted in a recent set of technical specifications adopted by the IETF that uses the acronym DNSSEC, which stands for Domain Name System Security Extension. Under DNSSEC, the IETF has proposed a suite of security add-on functionalities that would become part of the accepted Internet Protocol. The new security features would allow a user to confirm the authenticity of a domain name and assure the data integrity of the domain name system (DNS). In other words, the DNSSEC protocols would allow users to be sure that when they attempt to connect to a domain name, such as "whitehouse.gov," they are reaching the whitehouse.gov website, and they have not been maliciously redirected to some phony facsimile.

Pursuant to DNSSEC, every website will have a certificate of authenticity that will verify that the site is, in fact, the site it purports to be. So, once DNSSEC is deployed, a "security resolver" function would be able to check the authenticity of the registration of the "chase.com" website that your browser is accessing and return to the user either a confirmation that the website is the real chase.com or a warning that its authenticity could not be verified.

Interfering with the Internet. So why is DNSSEC relevant to a discussion of SOPA and PIPA? Those bills are intended to stop online piracy, but instead of attacking the pirates directly—mostly because they are offshore and outside U.S. jurisdiction—SOPA and PIPA look at Internet Service Providers (ISPs) like Verizon and use them as the enforcement mechanism. Both SOPA and PIPA would allow the Attorney General to secure court orders that would require ISPs to prevent Internet traffic from going to pirating websites.

These bills would essentially allow the Attorney General to order ISPs to do something similar to what DNSSEC is trying to prevent: blocking an attempt to reach a website. From the browser code perspective, there is no practical difference between blocking access to the real chase.com and redirecting it to a phony one and blocking access to the real (but criminal) freeillegaldownloads.com—they are nearly identical operations.

To be sure, some differences remain. The latest versions of SOPA and PIPA (which used to have a "block and redirect" requirement but now have only a "block access" requirement) are slightly improved in that they no longer function exactly like criminals do. But they are still close enough to be troublesome. For one thing, the blocking function is likely to slow down domain-name resolution for the entire Internet. It will doubtless begin to erode the level of trust needed in the DNS system. And if American law establishes the principle of permitting DNS filtering, other countries will as well, and the concept of a universal addressing system will be degraded.

More fundamentally, if you disrupt the DNS resolution system, then…you disrupt it. We can really have no idea of the extent of the consequences of mandating the "block only" capability. But adding that functionality—so that an ISP can, when ordered by a court, disregard the basic directions of the DNS system—would only add complexity to the Internet addressing function and make it more likely that malicious efforts to "block and redirect" traffic would succeed. Any "blocking" function would, at a minimum, interfere with the anticipated operation of DNSSEC, complicating its ability to enhance security.

Would SOPA Even Accomplish Its Goal? Adding to their other problems, SOPA and PIPA simply would not work. Even if the Attorney General obtained a blocking order that stopped Verizon from letting one go directly to a pirate website, it

is relatively easy to work around the block. We can reasonably predict that a host of redirector domains would soon spring up, many of them linked to ISPs outside the United States and outside the Attorney General's jurisdiction. And after that, there would be downloadable program applications to get to those redirectors. Indeed, one such program, known as "DeSOPA," has already been developed and deployed as a proof of concept effort and can be downloaded as a Mozilla Firefox extension.

One expert from Sandia labs has called the DNS filtering mandates of SOPA and PIPA a "whack-a-mole" approach.[1] The requirements are sufficiently easy to evade that one can almost predict that the next iteration of PIPA or SOPA will try to make writing, downloading, and using programs to avoid a SOPA/PIPA mandate illegal. That is an effort doomed to failure.

Perhaps most importantly, however, these bills put Congress in the business of managing an integral function of the Internet in ways that are likely to have unanticipated consequences. A working domain-name system is like a working mailing address—the rest of the system depends on it. If the addressing system is compromised, apps will not work, queries will not be answered, and emails will not be received. All those depend on domain names being resolved in the right way. Once you go down the road of allowing (or ordering) the functionality of domain-name filtering (even for a "good" purpose), you create the potential for restricting domain-name access for a host of other purposes.

The underlying principle is known as "domain name universality"—the idea that all of the addressing routers on the system, no matter where they are, will take you to the same domain address for a given website. Everything about Internet communication is based on this principle, and one consequence of PIPA and SOPA is that the principle would be called into question. As a group of leading technology experts (some of whom actually built the Internet) stated:

> Mandated DNS filtering would be minimally effective and would present technical challenges that could frustrate important security initiatives. Additionally, it would promote development of techniques and software that circumvent use of the DNS. These actions would threaten the DNS's ability to provide universal naming, a primary source of the Internet's value as a single, unified, global communications network.... DNS filtering will be evaded through trivial and often automated changes through easily accessible and installed software plugins. Given this strong potential for evasion, the long-term benefits of using mandated DNS filtering to combat infringement seem modest at best.[2]

Or, as Dr. Leonard Napolitano of Sandia Labs put it in his letter to Congress, the bills: "1) are unlikely to be effective, 2) would negatively impact U.S. and global cybersecurity and Internet functionality, and 3) would delay the full adoption of DNSSEC and its security improvements over DNS."

Good Intentions, but Dangerous Flaws. SOPA and PIPA would not work; to the extent that they did, they would make Internet security protocols like DNSSEC more difficult to implement; and, at their core, the bills violate the fundamental principle of universality that makes the Internet function as a global communications system.

Late last week, Senator Patrick Leahy (D–VT), chairman of the Senate Judiciary Committee and one of the sponsors of PIPA, indicated that he would consider removing the DNS blocking provisions from the bill and "study" the matter further. Though the inefficacy of DNS blocking probably needs no further study, his statement is a welcome recognition of the problematic nature of these pro-

1. Leonard M. Napolitano, Jr., Sandia Labs, letter to Representative Zoe Lofgren (D–CA), November 16, 2011, at *http://www.scribd.com/doc/73106069/Napolitano-Response-Rep-Lofgren-11-16-11-c* (January 11, 2012).
2. Steve Crocker *et al.*, "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," May 2011, at *http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf* (January 11, 2012).

visions which, unfortunately, remain a part of the House version, SOPA.

One final point is not a technical argument, but a powerful policy principle: If the Chinese or Russians were proposing to do this to prevent access to dissident websites, the U.S. would be screaming bloody murder, and rightly so. Yet if this functionality were deployed, the ease with which censorship could occur would increase, and the United States would lose some of its moral authority to oppose information censorship. America has been struggling internationally to prevent the discussion of "cybersecurity" from mutating into a discussion of restricting Internet content—and these bills go in the opposite direction.

*—**Paul Rosenzweig** is a Visiting Fellow in the Center for Legal and Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*