

WebMemo



Published by The Heritage Foundation

No. 3438

December 21, 2011

Online Piracy and SOPA: Beware of Unintended Consequences

James L. Gattuso

It is one of the most contentious but least understood issues now before Congress—one that does not align neatly along party lines and has split the business community. The issue is online piracy, the illegal sale of copyrighted and trademarked products on rogue pirate websites. Since last week, the House Judiciary Committee has been struggling with legislation called the Stop Online Piracy Act (SOPA) or H.R. 3261, sponsored by committee Chairman Lamar Smith (R-TX). The bill would strengthen restrictions on foreign-based rogue websites, while imposing new obligations on U.S.-based firms that facilitate their operation. The legislation addresses a legitimate problem, but it may have unintended negative consequences for the operation of the Internet and free speech. Congress should carefully consider these factors before moving forward with any legislation.

Rogue Sites. There is no doubt that online piracy is a real problem. Websites selling counterfeit goods, including tangible items, such as branded clothing and pharmaceuticals, and digital goods, such as Hollywood movies, have proliferated on the Internet. Such activity is a form of theft, and the federal government has a legitimate role in preventing it. Currently, U.S. authorities can, and do, shut down domestically based “pirate” websites by seizing control of their domain names under asset-forfeiture laws.¹ But a large number of rogue sites are located

outside the United States, putting them largely out of the reach of U.S. authorities.

SOPA is intended to undercut such rogue sites by prohibiting third parties from enabling their activity.²

Lawsuits Authorized. As it is currently drafted, this is how SOPA would work: First, it allows the U.S. Attorney General, as well as individual intellectual property holders, to sue allegedly infringing sites in court. The site would have to be proven to be a foreign site “directed towards” the U.S. and that it would be subject to seizure if it were U.S.-based. Alternatively, a suit could be brought by a private plaintiff, who would have to show that the site is “dedicated to theft of U.S. property.” That test, in turn, can be met if the site or a portion of the site is “primarily” designed, operated, or marketed to “enable or facilitate” infringement. The bill requires that attempts be made to notify the website operator of any such legal action, but legal proceedings would go forward even if no response is received.

This paper, in its entirety, can be found at:
<http://report.heritage.org/wm3438>

Produced by the Thomas A. Roe Institute
for Economic Policy Studies

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

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

If the court finds in favor of the plaintiff, a range of third-party restrictions would go into effect. Specifically, in cases brought by the Attorney General, to the extent “technically feasible and reasonable,” a court order would:

1. Require Internet service providers to prevent subscribers from reaching the website in question. This would be done by severing the mechanism by which the domain name entered by Web users is connected (“resolved”) to the proper IP address;
2. Prohibit search engines such as Google from providing direct links to the foreign website in search results;
3. Prohibit payment network providers, such as PayPal or credit card firms, from completing financial transactions affecting the site; and
4. Bar Internet advertising firms from placing online ads from or to the affected website.

In cases brought by a private party, only the restrictions on payment networks and advertising firms would apply.

The current version of the legislation, offered as a manager’s amendment in committee, omits a number of controversial provisions that were included in prior versions of SOPA. Most notably, a process that allowed holders of intellectual property rights to trigger third-party obligations without a court

order was dropped. This and other recent changes represent a real improvement in the legislation.

Security Concerns. Yet, a number of serious and legitimate concerns remain. Foremost among these is the potential negative effect on Internet security. A number of concerns have been raised. One is that, by blocking “resolution” of IP addresses by servers in the U.S., users (and their browsers) would instead use less secure servers elsewhere to continue accessing blocked sites. Some have also said such domain-name filtering could disrupt access to other, non-infringing domain names.³ There are also concerns that SOPA could interfere with deployment of a newly developed Internet security system known as “DNSSEC” (which is intended to ensure the successful “resolution” of IP addresses), further weakening security.⁴

SOPA would undercut other policy goals as well. The requirement that search engines omit links to rogue sites undercuts the role of search firms as trusted intermediaries in conveying information to users. There are, of course, other circumstances where search engines already omit information and links—for instance, Google routinely screens out child pornography from its search results. But there has never been a government mandate that information be withheld from search results. Imposing such a mandate would represent the first step down a classic slippery slope of government interference that has no clear stopping point.

1. See John P. Mello, Jr., “Feds Celebrate Cyber Monday With Crackdown on Counterfeiters,” PC World, November 28, 2011, at http://www.pcworld.com/article/245045/feds_celebrate_cyber_monday_with_crackdown_on_counterfeiters.html?tk=rel_news (December 21, 2011). This authority is itself not without controversy. See Mike Masnick, “Feds Falsely Censor Popular Blog For Over a Year, Deny All Due Process, Deny All Details,” Techdirt, December 8, 2011, at <http://www.techdirt.com/articles/20111208/08225217010/breaking-news-feds-falsely-censor-popular-blog-over-year-deny-all-due-process-hide-all-details.shtml> (December 21, 2011).
2. A similar but not identical bill, the Protect IP Act (S. 968), is pending in the Senate.
3. Dr. Leonard M. Napolitano, Jr., Director, Computer Sciences and Information Services, Sandia National Laboratories, Letter to The Honorable Zoe Lofgren, November 16, 2011, at <http://www.scribd.com/doc/73106069/Napolitano-Response-Rep-Lofgren-11-16-11-c> (December 21, 2011).
4. See Stewart Baker, “SOPA-Rope-a-dope,” The Volokh Conspiracy, December 14, 2011, at http://volokh.com/2011/12/14/sopa-rope-a-dope/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+volokh%2Fmainfeed+%28The+Volokh+Conspiracy%29 (December 21, 2011).

Arguably, the limits placed on search engines as well as other third parties under SOPA would also violate constitutional protections of freedom of speech.⁵ But even if not barred legally, any such restrictions should be imposed only after the most careful consideration, only when absolutely necessary, and even then, to the smallest degree possible.

While the legislation's goal—the protection of property—is a proper one, there are alternative approaches. One potential alternative was recently outlined in a proposal by Senator Ron Wyden (D-OR) and Representative Darrell Issa (R-CA) to expand the jurisdiction of the International Trade Commission's copyright and trademark enforcement authority to include imports of digital goods as well as physical products. That would not address

all of the problems with foreign rogue websites, particularly producers of non-digital goods. But the Wyden–Issa approach would make it possible to impose reasonable limits on third-party assistance to rogue sites, under established rules.⁶

Consider Legislation Carefully. The federal government needs to protect intellectual property rights. But it should do so in a way that does not disrupt the growth of technology, does not weaken Internet security, respects free speech rights, and solves the problem of rogue sites. Congress should carefully consider the consequences of and alternatives to the legislation before moving forward.

—James L. Gattuso is Senior Research Fellow in Regulatory Policy in the Thomas A. Roe Institute for Economic Policy Studies at The Heritage Foundation.

-
5. At least one legal scholar maintained that the previous version of the bill did violate the First Amendment. See Lawrence H. Tribe, “The ‘Stop Online Piracy Act’ (SOPA) Violates the First Amendment,” Center for the Study of Innovative Freedom, December 6, 2011, at <http://c4sif.org/2011/12/tribe-sopa-is-unconstitutional/> (December 21, 2011).
 6. Gautham Nagesh, “Rep. Issa, Sen. Wyden Announce Competing Bill to Judiciary’s Stop Online Piracy Act,” The Hill, December 8, 2011, at <http://thehill.com/blogs/hillicon-valley/technology/198135-issa-wyden-unveil-competing-online-piracy-bill> (December 21, 2011).