



The Center for
Internet and Society

What's Wrong With SOPA?

December 7, 2011

Contents

- 1-6 Overview of the Overview of the Stop Online Piracy Act (SOPA)

- 7-8 Fighting the Unauthorized Trade of Digital Goods While Protecting Internet Security, Commerce and Speech

- 9 Download Paul Vixie's whitepaper "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill"

Overview of the Stop Online Piracy Act (SOPA)

TITLE I – Combating Online Piracy

Section 102

Initiator:	Attorney General
Target:	<p>“foreign infringing [web]sites” (domains with neither a registrar nor registry in the USA, e.g., most country code top-level domains such as .uk)</p> <ul style="list-style-type: none">• site is directed at U.S.• Committing or facilitating criminal infringement (e.g., willful infringement for commercial gain or valued at more than \$1000)• Subject to seizure if it were domestic• DMCA safe-harbor compliance is no defense
Mechanism:	<p>Attorney General files suit and obtains temporary restraining order, preliminary injunction, or other injunction preventing site from “undertaking any further activity as a foreign infringing site.” Order can then be served on U.S. intermediaries.</p>
Proof:	None specified.
Consequences:	<p>Within five days of being served with notice of order:</p> <p><u>Service Providers</u> must “take technically feasible and reasonable measures designed to prevent access ... to foreign infringing site” including preventing domain name from resolving to IP address.</p> <ul style="list-style-type: none">• Explicitly preserves DMCA section 512 safe-harbor.• Duty to monitor unspecified. <p><u>Search Engines</u> must “take technically feasible and reasonable measures . . . to prevent the foreign infringing site . . . from being served as a direct hypertext link.”</p> <ul style="list-style-type: none">• Does not preserve DMCA section 512 safe-harbor.• Duty to monitor is unspecified. <p><u>Payment Network Providers</u> must “take technically feasible and reasonable measures . . . to prevent, prohibit, or suspend . . . transactions” between their U.S. customers and the foreign infringing site.</p> <ul style="list-style-type: none">• Termination obligation limited to accounts as of date order is served.

Consequences: Within five days of being served with notification (unless counter-notice is received):

Payment Network Providers must “take technically feasible and reasonable measures . . . to prevent, prohibit, or suspend . . . transactions” between their U.S. customers and the foreign infringing site.

Internet Advertising Services must “take technically feasible and reasonable measures” to “prevent its service from providing advertisements . . . relating to the foreign infringing site” and stop providing or receiving any compensation for advertising services relating to that site.

Counter-Notice: Targeted site may serve counter-notice consenting to jurisdiction of U.S. Courts. Suspends duties of Payment Network Providers and Internet Advertising Services.

Judicial Relief: Upon counter-notice, copyright or trademark owner may then commence suite against the registrant of the domain name or the site’s owner or operator, or in rem against the site or domain. May obtain same injunctive relief specified in Section 102.

Service of injunction order on Payment Network Providers and Internet Advertising Services triggers same general obligations as specified in Section 102. Copyright or trademark owner may enforce obligations through action for injunctive relief. Same defenses and immunities apply as specified in Section 102.

Section 104

Service providers (defined as any provider of online services), payment network providers, Internet advertising services, advertisers, search engines, domain name registries, and domain name registrars who block access or terminate financial affiliation voluntarily are immunized from suit and liability if they reasonably believe a site is a “foreign infringing site” or is “dedicated to theft of U.S. property.”

Section 105

Immunizes service providers, payment network providers, Internet advertising services, advertisers, search engines, domain name registries, and domain name registrars from suit if they refuse to provide services to any Internet site that “endangers public health.” A site “endangers public health” if it sells prescription drugs without requiring a prescription or sells drugs that are “misbranded” within the meaning of the FDCA.

3. Forfeiture

Existing law provides for criminal forfeiture of “[a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of” criminal copyright infringement. *See* 18 U.S.C. § 2323. This provision does not require that the owner or operator of the property subject to seizure be aware of the violation. By criminalizing “public performances” via a “computer network,” SOPA leaves any part of the relevant computer network subject to seizure by the government—even if the owner is unaware of the violation.

Section 202

Adds intentionally importing, exporting or trafficking in “counterfeit drugs” to the offenses listed in 18 U.S.C. §2320. Also adds a subsection creating criminal penalties for knowingly trafficking in goods that are “falsely identified as meeting military standards.”

Section 203

Increases the criminal penalties for international economic espionage under 18 U.S.C. § 1831.

Section 204

Directs the United States Sentencing Commission to “review, and if appropriate, amend” the Sentencing Guidelines relating to intellectual property offenses. The Commission is directed to consider whether the Guidelines should incorporate various factors such as whether an offense was “committed in connection with an organized criminal enterprise” or involved international “economic espionage.”

Section 205

Directs the Secretary of State and the Secretary of Commerce, in consultation with the Register of Copyrights, to “ensure that the protection in foreign countries of the intellectual property rights of United States persons is a significant component of United States foreign and commercial policy in general, and in relations with individual countries in particular.”

Requires the appointment of an “intellectual property attaché” to at least one embassy within every region covered by a regional bureau of the Department of State. Encourages the Secretary of State to appoint these attachés to countries that have been identified as raising IP enforcement priorities for the United States.

Fighting the Unauthorized Trade of Digital Goods While Protecting Internet Security, Commerce and Speech

Draft framework for discussion, authored by: U.S. Senators Cantwell, Moran, Warner and Wyden and U.S. Representatives Chaffetz, Campbell, Doggett, Eshoo, Issa, Lofgren and Polis

BACKGROUND

While the Internet has been revolutionary when it comes to uniting communities, promoting ideas and creating boundless opportunities for innovation and commerce, the Internet has also created new avenues for foreign counterfeiters and others operating outside the United States to sell unauthorized goods on the American market. This is harmful to the legitimate rights holders operating and employing Americans here at home.

Downloading a movie from a foreign-registered site, for example, is much like importing a good from a foreign company; however U.S. trade laws – put in place to oversee the flow of goods and services into the United States – have failed to keep up with the digital economy. A 21st Century trade policy will combat the import of infringing digital goods and counterfeit merchandise while ensuring the continued free flow of legitimate commerce and speech online.

We found that using trade laws to address the flow of infringing digital goods into the United States makes it possible to avoid many of the pitfalls that would arise from other legislative proposals currently being advanced to combat online infringement. Namely by putting the regulatory power in the hands of the International Trade Commission – versus a diversity of magistrate judges not versed in Internet and trade policy – will ensure a transparent process in which import policy is fairly and consistently applied and all interests are taken into account. When infringement is addressed only from a narrow judicial perspective, important issues pertaining to cybersecurity and the promotion of online innovation, commerce and speech get neglected. By approaching digital good infringement as a matter of regulating international commerce, we are able to take all of these factors into account.

PROPOSAL

This proposal updates import laws to respond to the challenges posed by the digital economy, so that illegal digital imports and digitally-facilitated imports of counterfeit goods are deterred. This proposal would enable a U.S. rightsholder to petition the International Trade Commission (ITC) to launch an investigation into the imports in question.

Congress established the independent International Trade Commission (ITC) as an arbiter of whether imports violate U.S. intellectual property rights and should or should not be allowed into the U.S. Under current law, rightsholders can petition the ITC to investigate whether

**Security and Other Technical Concerns Raised by the DNS Filtering Requirements
in the PROTECT IP Bill**

Authors:

Steve Crocker, Shinkuro, Inc.

David Dagon, Georgia Tech

Dan Kaminsky, DKH

Danny McPherson, Verisign, Inc.

Paul Vixie, Internet Systems Consortium

Download Whitepaper: <http://bit.ly/sZBJbd>