



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"><li>• site is directed at U.S.</li><li>• Committing or facilitating criminal infringement (e.g., willful infringement for commercial gain or valued at more than \$1000)</li><li>• Subject to seizure if it were domestic</li><li>• DMCA safe-harbor compliance is no defense</li></ul>
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><b><u>Service Providers</u></b> 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"><li>• Explicitly preserves DMCA section 512 safe-harbor.</li><li>• Duty to monitor unspecified.</li></ul> <p><b><u>Search Engines</u></b> 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"><li>• Does not preserve DMCA section 512 safe-harbor.</li><li>• Duty to monitor is unspecified.</li></ul> <p><b><u>Payment Network Providers</u></b> 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"><li>• Termination obligation limited to accounts as of date order is served.</li></ul>

**Internet Advertising Services** must “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.

- Termination obligation limited to accounts as of date order is served.

Enforcement: Only the Attorney General may enforce the above through injunctive relief. Provides defense for technical inability, or unreasonable economic burden.

Immunity: Provides immunity from suit and liability to intermediaries for “any act reasonably designed to comply” with obligations imposed above.

### **Section 103**

Initiator: Owner of any intellectual property right harmed by the targeted site

Target: Internet sites “dedicated to the theft of U.S. property”

- Domestic or foreign sites
- Directed at U.S. and meets one of the following:
  - (i) primarily designed or operated for the purpose of enabling or facilitating any copyright infringement, violation of DMCA anti-circumvention provisions, or Lanham Act counterfeiting; or
  - (ii) takes “deliberate actions to avoid confirming a high probability” of copyright infringement or violation of DMCA anti-circumvention provisions; or
  - (iii) operates the site with the object of promoting copyright infringement or violation of DMCA anti-circumvention provisions.
- DMCA safe-harbor compliance is no defense

Mechanism: Private party serves notification directly on intermediaries identifying site as one “dedicated to the theft of U.S. property” and providing “specific facts” that support that claim as well as a threat of “immediate and irreparable injury loss, or damage.”

Proof: None specified.

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.

## **Section 106**

Directs the Attorney General to develop internal procedures regarding SOPA and to publish guidance for the public. Requires the Register of Copyrights to conduct a study on the effectiveness of SOPA.

## **Section 107**

Directs the Intellectual Property Enforcement Coordinator, in consultation with a variety of government departments, to conduct a study and report to Congress regarding whether United States law should be reformed so as to prohibit “notorious foreign infringers” from raising capital in the United States.

## **TITLE II – Additional Enhancements to Combat Intellectual Property Theft**

### **Section 201**

Expands the range of copyright infringement subject to criminal penalties.

#### **1. Criminal sanctions for streaming:**

Imposes criminal sanctions for “public performances” via “computer network” (i.e. streaming). A single public performance where “the total retail value . . . of the public performances, is more than \$1,000” can be a misdemeanor. These criminal sanctions can be applied even if the public performance was not for private commercial gain.

Felony penalties (including up to 3 years imprisonment) apply for “10 public performances by means of digital transmission, of 1 or more copyrighted works, during any 180-day period, which have a total retail value of more than \$2,500 . . . .” Again, the value of the work allegedly infringed, and not commercial gain to the alleged infringer, determines whether the public performance is a felony.

#### **2. New construction of “willfully”**

Criminal copyright provisions only apply where a person “willfully infringes” copyright. 17 U.S.C. § 505(a)(1). The current statute does not define “willfully”—it is generally construed as requiring a knowing violation of the law.

Section 201(c) of SOPA includes a new rule of construction: a person with “a good faith reasonable basis in law to believe that the person’s conduct is lawful shall not be considered to have acted willfully for purposes of the amendments made by this section.” By implication, a person who believed her conduct was protected (e.g. fair use) might be found to have acted “willfully” if her belief about the law is held to be unreasonable.

### **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 21<sup>st</sup> 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

certain imports violate U.S. trademarks and copyrights. The ITC is authorized to not only investigate these issues but to initiate actions to prevent the imports in question from entering into the U.S.

Under our proposal, the ITC would be authorized to initiate an investigation at a rightsholder's request and issue a cease-and-desist order against foreign websites that provide illegal digital imports and/ or facilitate the importation of counterfeit goods. In order to issue such an order, the ITC would need to find that the foreign website is "*primarily*" and "*willfully*" engaging in infringement of U.S. copyrights or willfully enabling imports of counterfeit merchandise. This standard comports with existing copyright and trademark law. An ITC cease-and-desist order would, under this proposal, compel financial transaction providers and Internet advertising services to cease providing financial and advertising services to the foreign website.

The procedures the ITC would use throughout an investigation under this proposal are similar to those the agency currently employs. The public would be notified of the investigation and respondents would have a right to be heard, as well other interested parties. Final ITC determinations could be appealed in U.S. court.

Additionally, this proposal would enable the ITC to boost its capacity to carry out this proposal, to issue expedited cease-and-desist orders when the urgent need for speed is demonstrated, and to prescribe sanctions for those that may try to abuse their rights under this proposal. The proposal would empower the ITC to issue temporary and preliminary cease-and-desist orders, when immediate action is necessary to prevent imminent harm to rightsholders.

Finally, this plan provides appropriate immunity for those entities that are complying with the ITC orders, including financial transaction providers and Internet advertising services that voluntarily refuse to provide services to foreign websites that endanger public health by supplying illicit prescription drugs.

We intend to make public a draft of the legislative text of this proposal in order to enable the public to provide us with feedback and counsel before the proposal is formally introduced in the House and the Senate.

**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>**