KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

THE STOP ONLINE PIRACY ACT: SUMMARY, PROBLEMS & IMPLICATIONS

This document summarizes and analyzes Title I of H.R. 3261, the "Stop Online Piracy Act," which would create new causes of action against a wide range of Internet sites for facilitating copyright or trademark infringement. Title I is the House companion to the Senate's PROTECT IP Act and shares that bill's significant problems; in addition, SOPA sweeps much more broadly and would chill online innovation and expression by creating major new litigation risks for service providers currently protected by the DMCA safe harbor.

Sec. 102 allows the government to impose new obligations on a range of intermediaries to block access to sites that facilitate criminal copyright or trademark infringement

This section defines new actions that may be brought by the U.S. Attorney General against a "foreign infringing site" or portion thereof. The court can then issue injunctions against the site to cease and desist further activity as a foreign infringing site.

Any site could be deemed a **"foreign infringing site"** if:

- its domain-name registration authorities are located outside the U.S.; and
- it so much as "*facilitates*" the commission of criminal copyright or trademark infringement.

Whether the site intended to foster infringement appears to be irrelevant, as is the amount of noninfringing expression on the site.

Once an order has issued against a site, the A.G. can serve a copy, with court approval, on any of several intermediaries, who must take action specified in the bill within 5 days or as ordered:

- **ISPs (and other online service providers that operate caching DNS servers)** must take measures designed to "prevent access" to the site (or portion thereof), including measures designed to prevent DNS resolution of the site's domain name;
- **search engines** must take measures designed to prevent the site (or portion thereof) from being served as links in search results;
- **payment networks** must take measures designed to prevent, prohibit, or suspend transactions between the site and US customers;
- **ad networks** must take measures designed to stop serving ads *on* the site, stop serving ads *for* the site (including sponsored links), and cease all compensation to or from the site.

Subsequently, the A.G. can bring actions against these intermediaries to compel compliance, and can seek injunctions against anyone who provides tools to circumvent the orders.

Sec. 103 creates a notice-and-cutoff system that allows private parties to target a website's financial resources

This section creates a private cut-off system, superficially modeled on the DMCA's notice-and-takedown system, for cutting off sites' financial resources. It requires that payment and ad networks cease doing business with any site within 5 days of receiving an *allegation* by a rightsholder that the site is "dedicated to theft of U.S. property" – using a definition of "dedicated" that is nothing like the common usage of the word. If the financial intermediary does not cease doing business with the site, either based on its own judgment or because it receives a counter-notice from the site, the rightsholder can initiate a lawsuit against the accused site. If the court agrees that the site meets the broad definition of "dedicated to theft," the site can be enjoined from operating in its current manner and payment and ad networks can be compelled to stop doing business with the site.

Any site could be deemed **"dedicated to theft of U.S. property"** if:

- it offers its service "in a manner that . . . enables or facilitates" infringement; or
- its operator takes or has taken "deliberate actions to avoid confirming a high probability" of infringing activity on the site.

It appears to be no defense that the site has extensive lawful uses; that its operator has done nothing to encourage infringing use; or that the site has complied with section 512 of the DMCA.

SOPA's Problems & Implications

DNS-filtering interferes with core Internet infrastructure and will have little effect on infringement. Altering DNS results as required under the bill causes significant problems for cybersecurity: It is inconsistent with DNSSEC, a key cybersecurity initiative, and circumvention of filters will expose U.S. users and networks to increased cybersecurity risk. At the same time, the filters will be trivial to circumvent, and will thus have too small and diminishing an impact on infringement to justify the cybersecurity costs. Where DNS filtering does have an effect, for technical reasons its impact is likely to be overbroad and result in blocking lawful expression rather than just infringement. Lastly, the adoption of technical tools that can be used for censorship sets a dangerous international precedent that conflicts with U.S. foreign policy goals. For more on these concerns, *see* CDT Warns Against Widespread Use of Domain-Name Tactics to Enforce Copyright [http://cdt.org/policy/cdt-warns-against-widespread-use-domain-name-tactics-enforce-copyright]

SOPA would impose new responsibilities on ISPs to scrutinize and screen all user traffic. In addition to DNS-filtering, SOPA would impose an open-ended obligation on ISPs to "prevent access" to infringing sites. Doing that would require ISPs to inspect the Internet traffic of its entire user base – the kind of behavior that has proved highly controversial in the context of "deep packet inspection" for advertising purposes. The obligation the bill would impose is also similar to that of a Pennsylvania statute overturned on constitutional grounds in *CDT v. Pappert*. For more on that case, *see* http://cdt.org/speech/pennwebblock/.

SOPA would chill the growth of social media and force sites to adopt a new role as content police. Under SOPA, general-purpose social media sites with no bad intent could be argued to "facilitate" infringement – and thus get tagged as theft sites – simply by virtue of providing the platforms for users' content. To protect themselves, platforms of all kinds would be pressured to actively monitor and police user behavior. The new de facto duty to track and control user behavior would significantly chill innovation in social media and undermine social websites' central role in fostering free expression. It would also set the dangerous international precedent that governments seeking to block online content that violates domestic law should look to online communications platforms as points of control.

Any online content or communications platform could lose its financial support at the whim of the most litigious rightsholder. Under SOPA, every user-generated content platform, social media website, or cloud-based storage service would be at constant risk of being cut off from payment or ad networks. All it would take to start the process – and put the website in serious jeopardy – is a single rightsholder alleging to the payment and ad networks that the challenged website is designed in a way that prevents it from sufficiently "confirming" infringement. In effect, every online communications platform would be at the mercy of not just mainstream rightsholders, but whatever rightsholder is the most aggressive and litigious.

The bill would eviscerate the predictable legal environment created by the DMCA, subjecting innovators to a new era of uncertainty and risk. User-driven sites have flourished under the DMCA safe harbor, which clearly defines their legal responsibilities and expressly rejects any obligation to actively track and police user behavior. Under SOPA, that legal predictability would be tossed aside. Every such site would be exposed to a constant risk of rightsholders and courts second-guessing the site's technical architecture, in challenges asserting that the site "facilitates" or "fails to confirm" infringement. Smaller, emerging services would be especially hard-hit by the resulting uncertainty.

For more information, contact:
David Sohn, dsohn@cdt.org
Andrew McDiarmid, andrew@cdt.org