November 15, 2011

The Honorable Lamar Smith
Chairman
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

The Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515

Re: H.R. 3261, the Stop Online Piracy Act

Dear Chairman Smith and Ranking Member Conyers,

The undersigned advocates and organizations write to express our deep concern with H.R. 3261, the "Stop Online Piracy Act" (SOPA). While we support appropriate copyright enforcement and want to ensure that creators around the world have the opportunity to be compensated for their works, SOPA as constructed would come at too high a cost to Internet communication and noninfringing online expression. The bill would set an irreversible precedent that encourages the fracturing of the Internet, undermines freedom of expression worldwide, and has numerous other unintended and harmful consequences.

We do not dispute that there are hubs of online infringement. But the definitions of the sites that would be subject to SOPA's remedies are so broad that they would encompass far more than those bad actors profiting from infringement. By including all sites that may – even inadvertently – "facilitate" infringement, the bill raises serious concerns about overbreadth. Under section 102 of the bill, a nondomestic startup video-sharing site with thousands of innocent users sharing their own noninfringing videos, but a small minority who use the site to criminally infringe, could find its domain blocked by U.S. DNS operators. Countless non-infringing videos from the likes of aspiring artists, proud parents, citizen journalists, and human rights activists would be unduly swept up by such an action. Furthermore, overreach resulting from bill is more likely to impact the operators of smaller websites and services that do not have the legal capacity to fight false claims of infringement.

Relying on an even broader definition of "site dedicated to theft of US property," section 103 of SOPA creates a private right of action of breathtaking scope. Any rightsholder could cut off the financial lifeblood of services such as search engines, user-generated content platforms, social media, and cloud-based storage unless those services actively monitor and police user activity to the rightsholder's satisfaction. A mere accusation by any rightsholder would be sufficient to require payment systems and ad networks to terminate doing business with the service; the accused service's only recourse would be to send a counter-notice, at which point it would be at the networks' discretion whether to reinstate the service's access to payments and advertising. This would bypass and effectively overturn the basic framework of the Digital Millennium Copyright Act (DMCA), by pushing user-driven sites like Twitter, YouTube, and Facebook to implement ever-more elaborate monitoring systems to "confirm," to the satisfaction of the most aggressive and litigious rightsholder, whether individual users are exchanging infringing content. These and other sites have flourished under the DMCA safe harbor, which provides certainty concerning the legal responsibilities of online service providers and expressly rejects a de facto legal obligation to actively track and police user behavior. Creating such an obligation would be hugely damaging to Internet innovation, particularly for smaller, emerging sites and individuals. It would also carry major consequences for users' legitimate privacy interests.

We also have serious concerns about the inclusion the provisions in section 102 to require ISPs to filter Domain Name System (DNS) requests or otherwise try to "prevent access" to targeted websites.[1] DNS-filtering is trivial to

[1] These concerns also apply to the DNS Filtering provisions included S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, also known as the PROTECT IP Act, which

circumvent and will be ineffective at stopping infringement. Where it does have an impact, that effect is likely to be overbroad, sweeping in legitimate online content. We have witnessed this already in the case of mooo.com, the seizure of which led to upwards of 84,000 innocent subdomains being blocked.[2]

In addition, mandated filtering would undermine the U.S. government's commitment to advancing a single, global Internet. Its inclusion risks setting a precedent for other countries, even democratic ones, to use the same mechanisms to enforce a range of domestic policies, effectively balkanizing the global medium of the Internet. Simply declaring that filtering aimed at copyright and trademark infringement is different from filtering with more sinister motives does not change the message this would send to the world – that the United States is legitimizing methods of online censorship to enforce its domestic laws. Non-democratic regimes could seize on the precedent to justify measures that would hinder online freedom of expression and association.

DNS-filtering also raises very real cybersecurity concerns.[3] It conflicts with Secure DNS (DNSSEC), and circumventing the filters will risk making domestic networks and users more vulnerable to cybersecurity attacks and identity theft as users migrate to offshore DNS providers not subject to filtering orders. Given the ease with which DNS filters can be circumvented, there is strong reason to doubt that its benefits are worth these costs.

The undersigned organizations recognize the importance of addressing truly illicit behavior online. We share the overall goals of many of SOPA's supporters – preventing large-scale commercial infringement and ensuring that creativity and expression thrive. Intellectual property infringement breaks the law online or off, but SOPA is not the right way to stop it. Current enforcement mechanisms were designed to avoid the countervailing harms of conscripting intermediaries into being points of control on the Internet and deciding what is and what is not copyright-infringing expression. As drafted, SOPA radically alters digital copyright policy in ways that will be detrimental to online expression, innovation, and security.

Sincerely,

American Library Association
Association of Research Libraries
Center for Democracy & Technology
Competitive Enterprise Institute
Demand Progress
Electronic Frontier Foundation
Freedom House
Human Rights First
Human Rights Watch
Internews
New America Foundation's Open Technology Initiative
Public Knowledge
TechFreedom

---

many of these organizations have also publicly opposed http://www.publicknowledge.org/Public-Interest-Letter-PROTECT-IP-Act.

[2] *See* Thomas Claburn, *ICE Confirms Inadvertent Web Site Seizures*, *Information Week*, February 18, 2011. http://www.informationweek.com/news/security/vulnerabilities/229218959?cid=RSSfeed_IWK_All.

[3] *See* Steve Crocker, David Dagon, Dan Kaminsky, Danny McPherson, and Paul Vixie, *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill*, May 2011 http://www.circleid.com/pdf/PROTECT-IP-Technical-Whitepaper-Final.pdf.