

House Copyright Bill Casts Dangerously Broad Net

by [David Sohn](#) [1]

October 27, 2011

CDT has argued for some time that the domain-name filtering provisions of the Senate's PROTECT IP Act [raise serious problems](#) [2]. Domain-name filtering is a blunt instrument; it is trivial to evade and hence won't be effective; it carries risks for cybersecurity; and it sets a bad international precedent; and it can inadvertently affect lawful speech. Infringement is a real problem, but trying to tackle it via the domain name system is a mistake.

Yesterday, key members of the House Judiciary Committee introduced a [bill](#) [3] (H.R. 3261, the "Stop Online Piracy Act") that not only repeats that mistake, but dangerously extends the scope. Gone is any serious effort to narrowly target clear "bad actors" and to craft legislation that seeks to root out the "worst of the worst" -- a phrase we have often heard from proponents of such legislation. In its place is a bill that appears to impose sweeping new risks and responsibilities on websites offering legitimate online services and to give rights holders a powerful new club to wield against any online service they believe isn't doing enough to police infringement. We are still analyzing the details (78 pages of statutory language is a lot to chew on), but our initial read is that the bill would mark a radical departure from core legal principles embedded in the DMCA and in secondary liability jurisprudence. Abandoning those principles would pose major risks for online innovation, free expression, and the open nature of the Internet.

A central issue is that the bill's definitions of bad websites are vague and broad. [As CDT noted](#) [4] when the PROTECT IP bill was introduced, that bill did a much better job than its 2010 predecessor of tailoring its definitions to target true bad actors. As a result, there was less potential for the bill to inadvertently sweep in legitimate websites.

H.R. 3261 goes the opposite direction. The definition of "foreign infringement site" includes not just sites that are dedicated to or even primarily focused on infringement, but rather any site that "facilitates" it. I see no requirement of bad intent. Nor is there any definition of what it means to "facilitate." When the user of a user-generated content website posts infringing material, has the website "facilitated" that infringement? When users store infringing material in a cloud-based data service, has the service "facilitated" the infringement? The definition leaves open the possibility that any non-U.S. website that enables communications by users could be treated as a "foreign infringement site" if even a single user employs the website in a manner constituting criminal copyright infringement.

'Backdoor' Monitoring Obligation

Another section of H.R. 3261 says that a website is "dedicated to theft of U.S. property" if (among several independent definitional prongs) it takes "deliberate actions to avoid confirming a high probability" of the use of the site to carry out copyright infringement. Not exactly a model of clarity. But the beauty of this provision, from the point of view of a rights holder, is that there is no need to go to court to puzzle through what this means. Instead, rights holders can decide for themselves. All they need is a good faith belief that a website is "avoiding confirming" infringement, and they can demand that payment systems and advertising networks cease doing business with the website. (Payment systems and ad networks are required to comply unless and until they receive a counter-notice, at which point they have discretion to reinstate the website pending a possible court order or just ignore the counter-notice and be done with it.)

This seems like a backdoor way of imposing a monitoring obligation on any website that allows users to post content. (Precisely what the DMCA, in 17 U.S.C. 512(m), expressly says is not required.) If any website sets itself up in a way that does not actively log or monitor user behavior, a rights holder can always allege that the site is "avoiding confirming" the use of the site for infringement. That rights holder allegation is sufficient to put the website at major risk of losing access to payment

and ad networks. In short, the definition appears to give any rights holder a major club with which to bludgeon any website or online service that the rights holder believes isn't doing enough to monitor copyright infringement. And keep in mind that we're not just talking about a limited number of major corporate rights holders; everyone is a copyright holder these days, and copyright trolls or aggressive litigants like Perfect10 are perfectly willing to shake down legitimate sites based on questionable allegations.

The bottom line is, by trying to sweep in virtually the entire Internet ecosystem, this new bill would do major damage. Narrowly targeting the true bad actors is one thing. Imposing major new costs and risks on anyone providing online communications tools would seriously undermine online innovation and free expression. Concern about online infringement is understandable, but Congress needs to take much greater care to avoid throwing out the baby with the bathwater.

-
- [Digital Copyright](#)

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://cdt.org/blogs/david-sohn/2710house-copyright-bill-casts-dangerously-broad-net>

Links:

[1] <https://cdt.org/personnel/david-sohn>

[2]

<http://www.cdt.org/policy/cdt-warns-against-widespread-use-domain-name-tactics-enforce-copyright>

[3] <http://judiciary.house.gov/hearings/pdf/112%20HR%203261.pdf>

[4] <http://www.cdt.org/protect-ip-act>