

SOPA (H.R. 3261) and PIPA (S. 968) Talking Points

There are several problematic areas with H.R. 3261, the *Stop Online Piracy Act* (SOPA) introduced by House Judiciary Chairman Lamar Smith (R-TX), and S. 968 the *Protect IP Act* (PIPA) introduced by Senate Judiciary Chairman Patrick Leahy. The three biggest concerns Public Knowledge has with the SOPA and PIPA bills are that they:

- 1. Gives intermediaries a fast-track to shutting down websites**
- 2. Creates conflict between Domain Name System (DNS) servers**
- 3. Sanctions government interference with the Internet**

The first concern deals with a private right of action provision that interferes with other areas of the law. This provision is a blanket immunity provision for almost anyone who decides to cut off a targeted site. Internet Service Providers (ISPs), registrars, registries, or any advertiser can cut off a website without fear of repercussion if they can claim a “reasonable belief” that the site was infringing or not doing enough to stop infringement. Additionally, this blanket immunity could potentially be used to allow an ISP to violate net-neutrality rules without being held accountable.

The second concern with SOPA and PIPA addresses more technical issues and would affect the very nature of Internet security. By creating a conflict between US DNS servers and global DNS servers, SOPA and PIPA would make computers and networks more vulnerable to hackers, identity theft, and cyber attacks. Service providers would be required by the government to prevent user access to sites targeted for online piracy (DNS filtering). This DNS filtering goes against a system already established by Internet engineers that addresses the issues of locking down website identities – DNSSEC. Through DNSSEC, a website will be given identification credentials by the same company that registers its Internet name. Under the new DNSSEC system, the browser won’t take the user to a site not verified by that organization’s particular credentials.

Were SOPA and PIPA to become law, they would require an ISP to alter their DNS in a way that runs counter to the goals of DNSSEC. Numerous Internet engineers and cybersecurity experts have raised these concerns. Furthermore, Rep. Dan Lungren, the Chairman of the Cybersecurity Subcommittee on the House Homeland Security Committee, expressed concern that none of these experts were called to testify before the Judiciary Committee during the hearing on SOPA.

Finally, SOPA sanctions government interference with the Internet. The tools that would be used to implement DNS filtering would be identical to those used in China and Syria for censorship purposes. Constitutional lawyers and free speech experts have raised concerns that the copyright provisions in SOPA fail to meet the fundamental constitutional test for First Amendment protection. The solutions provided in this legislation threaten to damage democratic discourse and dissent in the US and would harm our ability to advocate on the merits of free speech internationally.

1818 N ST NW, Washington D.C. 20036