November 15, 2011

The Honorable Lamar Smith
Chairman
Committee on the Judiciary
House of Representatives
Washington, DC 20515

The Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary
House of Representatives
Washington, DC 20515

The Honorable Bob Goodlatte
Chairman
Subcommittee on Intellectual Property,
Competition, and the Internet
Committee on the Judiciary
House of Representatives
Washington, DC 20515

The Honorable Mel Watt
Ranking Member
Subcommittee on Intellectual Property,
Competition, and the Internet
Committee on the Judiciary
House of Representatives
Washington, DC 20515

Dear Chairman Smith and Representatives Conyers, Goodlatte, and Watt:

We write to express our concerns with H.R. 3261, the Stop Online Piracy Act. As consumer groups, we agree that consumers should not be harmed by substandard or counterfeit goods. However, we are concerned that some of the measures proposed by this bill and the breadth of its scope could make it more likely to harm consumers' interests. In particular, we are worried the bill could close off online exchanges that provide lower prices for consumers; reduce online security; and allow for anti-consumer practices by online service providers.

Consumer access to online exchanges

Consumers benefit greatly from being able to use the Internet to connect with a wide variety of buyers, sellers, and with each other. Online forums and marketplaces allow consumers to exchange information about products and exchange products themselves in thriving secondary markets. However, the broad language of the bill threatens these activities.

The bill would allow rights holders to send notices to payment processors and advertising networks, ordering them to cut off funding to sites the rights holders believe are "dedicated to the theft of U.S. property." However, this definition is extremely broad. Section 103(a)(1)(B)(ii) defines a "site dedicated to the theft of U.S. property" as including any site whose owner "takes active steps to avoid confirming a high probability" that it is being used (even by others) for infringement. This means that an entirely legitimate site can be defunded, and even enjoined entirely, merely because a few of its users may have infringed. Consequently, overzealous rights holders could shut down lawful exchange sites like craigslist, eBay, swap.com, or BookCrossing, closing off valuable outlets for small-scale buying and selling. For instance, a legitimate student-to-student textbook exchange site could be hampered or shut down by a publisher for the actions of just a few infringing users, raising the costs of an already-expensive education.

Online Security

Secure online communication and commerce is also of critical importance to consumers. Yet, the bill could undermine the security of consumers. Section 102(c)(2)(A) allows for court orders that would block domain name system (DNS) operators from providing access to the Internet Protocol (IP) addresses of targeted sites. In other words, a consumer attempting to access an allegedly infringing site would get an error message or be redirected to another page. However, redirecting DNS queries (to phishing sites and other fraudulent websites) is also a common tactic used by malicious hackers to steal millions of dollars from consumers.

To prevent these tactics, DNSSEC, an important voluntary security standard, is being implemented to ensure that any given DNS query will only return the correct, IP address. However, DNSSEC cannot tell the difference between DNS errors caused by these tactics or by court orders. This means that an ISP cannot simultaneously implement the consumer protections of end-to-end DNSSEC and obey court orders issued under SOPA. ISPs faced with this dilemma may well choose not to implement DNSSEC fully, leaving consumers more vulnerable online.

Furthermore, even under the bill's provision, users could still get to allegedly infringing sites. The simple steps infringers can take to do this, like downloading certain browser plugins or using questionable alternate DNS servers, exposes not only them, but all other consumers, to harm. These considerations mean that DNS blocking is not only largely ineffective, but risks seriously harming consumers' security.

Anti-consumer actions by online service providers

Finally, the bill grants complete immunity to a very large class of actors, including Internet service providers, advertising networks, advertisers, search engines, and payment networks, for cutting off access to a targeted site as long as they can claim their actions were taken in the reasonable belief that the site was suspected of encouraging infringement. This blanket immunity from all federal and state laws and regulations could allow the above actors to act in ways that would harm consumers. For example, Internet service providers could block access to online services that compete with their own telephone or video offerings under a justification of curbing alleged infringement, depriving consumers of legitimate alternatives to high-priced services. The broad immunity of the statute would prevent consumers or consumer protection agencies from policing or addressing such anti-consumer or anticompetitive.

As drafted, the Stop Online Piracy Act has the potential to do more harm to consumers than good. We urge you to reconsider these provisions as you continue to work on the important issue of protecting consumers online.

Respectfully submitted,

Consumer Federation of America
Consumers Union
U.S. PIRG: The Federation of State PIRGs