Common Misconceptions About The Stop Online Piracy Act and the Protect IP Act

The Stop Online Piracy Act (SOPA) (HR 3261) and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (Protect IP Act or PIPA) (S 968) are bills aimed at eliminating content piracy that have been the subject of much discussion in recent weeks. Votes will occur soon in the Senate and in the House, so the issue is worthy of your attention.

No one favors the theft of intellectual property. Voting against SOPA and/or PIPA is not a vote in favor of online piracy; no entity opposing these bills endorses content piracy in any way shape or form.

There is a fundamental misunderstanding of the adverse effect these bills would have on free speech that outweighs any possible curtailment of content piracy. These errors are, in and of themselves, evidence that the bills need significantly more review, discussion and understanding before they pass the House and Senate. We hope that you agree and, if so, that you will use any opportunities you have during the current Congressional recess to convey to your Members of Congress that these bills should not be rushed through Congress. While we prefer a vote against SOPA and PIPA, even a Senator's vote against invoking cloture on the bill and forcing legislators to engage in a thorough review of these issues would be helpful.

To that end, here are six basic facts about the Protect IP Act and SOPA you should know:

1. These bills are supposed to target just foreign sites but U.S.-based companies will end up taking the brunt of the collateral damage. Under these bills the Justice Department can order an Internet Service Provider ("ISP") to proactively block access to any site it deems as "rogue." Should the ISP not comply, it is in danger of serious financial and legal repercussions. Search engines can be made to strip the name of any offending site from its database and is liable for the same financial and legal penalties as ISPs if they don't comply. In addition, U.S. based companies with foreign operations, such as YouTube in the UK or Turkey or wherever, are at risk.

2. First Amendment Issues. The bills have the right intention – trying to address the issue of online piracy – but they are overbroad and will cause more harm than good. The blocking and/or seizure of websites allowed by these bills would almost certainly affect lawful speech. For example, when SOPA or PIPA authorized actions are taken against domain-names affiliated with websites containing a mix of lawful and unlawful content, all the content is affected; there is no way to narrowly target the unlawful content only. A concrete example occurred in last February, when the Department of Homeland Security mistakenly seized the domain “mooo.com.” As a result, many small, legitimate websites had their traffic redirected to a banner announcing that the domain had been seized for violating child pornography laws. It took a year to resolve the situation.

3. The manner in which ISPs and search engines will have to comply with an order to block access to certain websites fouls up the inner workings of the Internet, akin to throwing sugar into a gas tank. The Internet runs smoothly based on a set of technical standards that verify that a website's address is valid. New security standards being put in place now help these technical standards from being "spoofed" by hackers and other thieves. Top technical experts have written about the dangers of simply "blocking" a user request from reaching its destination and sending that request into some kind of cyberspace black hole. The new security standards can't be effective under these circumstances. User attempts to circumvent these blocking routines will lead that user to employ alternative domain name services, thus blocking an ISP's ability to observe and track cybersecurity threats on their networks. In addition, it would put users at the mercy of potentially unscrupulous foreign DNS servers, which could redirect user traffic for phishing or other nefarious purposes.

4. These bills raise human rights concerns as well. Enshrining domain-name seizure and blocking into law would give foreign governments political cover to take similar action, harming U.S. interests and undercutting diplomatic efforts to promote global Internet freedom. Following the U.S. example, other countries could try to seize or block the domain names of U.S. websites that are lawful here but that are asserted to violate some foreign law. In the case of domain-name seizure, such action could render the targeted domain inaccessible for the entire world. Setting such a precedent would also undermine US diplomacy. Over forty countries (and growing) now filter the Internet to some degree, and even liberal democracies are considering mandatory filtering and blocking regimes. Historically, the United States has been the strongest global voice against such balkanization of the Internet; the concept of a single, global Internet is a cornerstone of U.S. foreign policy on Internet matters. If the United States were to set the precedent that any country can order the blocking of a domain name if some of the content at that domain violates the country's laws, it is hard to see what credibility the U.S. would have as it urges other countries not to block access wherever they see fit.

5. As a result of those and other objections, a large bipartisan coalition has emerged to oppose the bills. Evidence of this is the Open Act, the bi-partisan alternative bill to SOPA and PIPA from Sen. Ron Wyden (R-OR) and Rep. Zoe Lofgren (D-CA) and Rep. Darrell Issa (R-CA). The Open Act attacks the online piracy problem by focusing carefully on true bad actors – sites whose function and purpose is to foster large-scale infringement. And once bad actors are identified, it takes the “follow the money” approach of cutting them off from payment and advertising networks, thus starving them of their financial lifeblood.

6. It Just Won't Work. Neither bill actually solves the intended problem of "shutting down" an infringing site. The bills call for either seizing a site or mandating that an ISP or search engine somehow prohibit users from accessing the site when typing in the common domain name, such as www.CNN.com. But neither seizing nor blocking a website's domain name actually removes the website – or any infringing content – from the Internet. The site and all its contents remain connected at the same IP address—the string of numbers the Internet's "address book" (the Domain Name Server or DNS) uses to connect a user to a particular website. If a site is seized, the site's operator merely has to buy another domain name and they are back in business. For example, most of the sports-streaming sites connected to ten domains ICE seized in February of 2011 quickly reappeared and are easily located at new domains.

   Users can easily find the IP address to any blocked site and type the numbers into their browser and make their way to the site. Web browser add-ons make this a trivial exercise, removing even the need to actually type in the numbers.