64 STAN. L. REV. ONLINE 34
December 19, 2011

DON'T BREAK THE INTERNET†

Mark Lemley,* David S. Levine,** & David G. Post***

Two bills now pending in Congress—the PROTECT IP Act of 2011 (Protect IP) in the Senate and the Stop Online Piracy Act (SOPA) in the House—represent the latest legislative attempts to address a serious global problem: large-scale online copyright and trademark infringement. Although the bills differ in certain respects, they share an underlying approach and an enforcement philosophy that pose grave constitutional problems and that could have potentially disastrous consequences for the stability and security of the Internet's addressing system, for the principle of interconnectivity that has helped drive the Internet's extraordinary growth, and for free expression.

To begin with, the bills represent an unprecedented, legally sanctioned assault on the Internet's critical technical infrastructure. Based upon nothing more than an application by a federal prosecutor alleging that a foreign website is "dedicated to infringing activities," Protect IP authorizes courts to order all U.S. Internet service providers, domain name registries, domain name registrars, and operators of domain name servers—a category that includes hundreds of thousands of small and medium-sized businesses, colleges, universities, nonprofit organizations, and the like—to take steps to prevent the offending site's domain name from translating to the correct Internet protocol address. These orders can be issued even when the domains in question are located outside of the United States and registered in top-level domains (e.g., .fr, .de, or .jp) whose operators are themselves located outside the United States; indeed, some of the bills' remedial provisions are directed solely at such domains.

Directing the remedial power of the courts towards the Internet's core technical infrastructure in this sledgehammer fashion has impact far beyond intellectual property rights enforcement—it threatens the fundamental principle of interconnectivity that is at the very heart of the Internet. The Internet's Domain Name System (DNS) is a foundational block upon which the Internet has been built and upon which its continued functioning critically depends; it is among a handful of protocols upon which almost every *other* protocol, and countless Internet applications, rely to operate smoothly. Court-ordered re-

* William H. Neukom Professor, Stanford Law School; Partner, Durie Tangri LLP.

** Assistant Professor, Elon University School of Law; Affiliate Scholar, Center for Internet and Society, Stanford Law School; Host, *Hearsay Culture* (KZSU-FM Stanford).

*** Professor, Beasley School of Law, Temple University.

moval or replacement of entries from the series of interlocking databases that reside in domain name servers and domain name registries around the globe undermines the principle of domain name universality—the principle that all domain name servers, wherever they may be located across the network, will return the same answer when queried with respect to the Internet address of any specific domain name. Much Internet communication, and many of the thousands of protocols and applications that together provide the platform for that communication, are premised on this principle.

Mandated court-ordered DNS filtering will also have potentially catastrophic consequences for DNS stability and security. It will subvert efforts currently underway—and strongly supported by the U.S. government—to build more robust security protections into the DNS protocols. In the words of a number of leading technology experts, several of whom have been intimately involved in the creation and continued evolution of the DNS for decades:

> Mandated DNS filtering would be minimally effective and would present technical challenges that could frustrate important security initiatives. Additionally, it would promote development of techniques and software that circumvent use of the DNS. These actions would threaten the DNS's ability to provide universal naming, a primary source of the Internet's value as a single, unified, global communications network. . . . DNS filtering will be evaded through trivial and often automated changes through easily accessible and installed software plugins. Given this strong potential for evasion, the long-term benefits of using mandated DNS filtering to combat infringement seem modest at best.[1]

Indeed, this approach could actually have an effect directly contrary to what its proponents intend: if large swaths of websites are cut out of the Internet addressing system, those sites—and the users who want to reach them—may well gravitate towards alternative, unregulated domain name addressing systems, making it even harder for governments to exercise their legitimate regulatory role in Internet activities.

The bills take aim not only at the Internet's core technical infrastructure, but at its economic and commercial infrastructure as well. Credit card companies, banks, and other financial institutions could be ordered to "prevent, prohibit, or suspend" all dealings with the site associated with the domain name. Online advertisers could be ordered to cease providing advertising services to the site associated with the domain name. Search engine providers could be ordered to "remove or disable access to the Internet site associated with the domain name," and to disable all hypertext links to the site.

These drastic consequences would be imposed against persons and organizations outside of the jurisdiction of the U.S. courts by virtue of the fiction that these prosecutorial actions are proceedings *in rem*, in which the "defendant" is

---

1. Steve Crocker et al., *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill*, DOMAININCITE.COM (May 2011), http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

not the operator of the site but the domain name itself. Both bills suggest that these remedies can be meted out by courts after nothing more than *ex parte* proceedings—proceedings at which only one side (the prosecutor or even a private plaintiff) need present evidence and the operator of the allegedly infringing site need not be present nor even made aware that the action was pending against his or her "property."

This not only violates basic principles of due process by depriving persons of property without a fair hearing and a reasonable opportunity to be heard, it also constitutes an unconstitutional abridgement of the freedom of speech protected by the First Amendment. The Supreme Court has made it abundantly clear that governmental action suppressing speech, if taken prior to an *adversary proceeding* and subsequent judicial determination that the speech in question is unlawful,[2] is a presumptively unconstitutional "prior restraint." In other words, it is the "most serious and the least tolerable infringement on First Amendment rights,"[3] permissible only in the narrowest range of circumstances. The Constitution requires a court "to make *a final determination"* that the material in question is unlawful "*after an adversary hearing before* the material is completely removed from circulation."[4]

The procedures outlined in both bills fail this fundamental constitutional test. Websites can be "completely removed from circulation"—rendered unreachable by, and invisible to, Internet users in the United States and abroad—immediately upon application by the government, without *any* reasonable opportunity for the owner or operator of the website in question to be heard or to present evidence on his or her own behalf. This falls far short of what the Constitution requires before speech can be eliminated from public circulation.

As serious as these infirmities are, SOPA, the House's bill, builds upon them, enlarges them, and makes them worse. Under SOPA, IP rights holders can proceed vigilante-style against allegedly offending sites, without *any* court hearing or any judicial intervention or oversight whatsoever. For example, SOPA establishes a scheme under which an IP rights holder need only notify credit card companies of the facts supporting its "good faith belief" that an identified Internet site is "primarily designed or operated for the purpose of" infringement. The recipients of that notice will then have five days to cease doing business with the specified site by taking "technically feasible and reasonable" steps to prevent it "from completing payment transactions" with customers. And all of this occurs based upon a notice delivered by the rights holder, which no neutral third party has even looked at, let alone adjudicated on the merits. If they get the assistance of a court, IP owners can also prevent other

2. Freedman v. Maryland, 380 U.S. 51, 58-60 (1965).

3. Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976).

4. Ctr. For Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 657 (E.D. Pa. 2004) (emphasis added).

companies from "making available advertisements" to the site, and the government can prevent search engines from pointing to that site.

These bills, and the enforcement philosophy that underlies them, represent a dramatic retreat from this country's tradition of leadership in supporting the free exchange of information and ideas on the Internet. At a time when many foreign governments have dramatically stepped up their efforts to censor Internet communications, these bills would incorporate into U.S. law a principle more closely associated with those repressive regimes: a right to insist on the removal of content from the global Internet, regardless of where it may have originated or be located, in service of the exigencies of domestic law.

United States law has long allowed Internet intermediaries to focus on empowering communications by and among users, free from the need to monitor, supervise, or play any other gatekeeping or policing role with respect to those communications. Requiring Internet service providers, website operators, search engine providers, credit card companies, banks, Internet advertisers, and others to block access to websites because of their content would constitute a dramatic retreat from that important policy. Laws protecting Internet intermediaries from liability for content on the Internet are responsible for transforming the Internet into the revolutionary communications medium that it is today. They reflect a policy that has not only helped make the United States the world leader in a wide range of Internet-related industries, but that has also enabled the Internet's uniquely decentralized structure to serve as a global platform for innovation, speech, collaboration, civic engagement, and economic growth. These bills would undermine that leadership and dramatically diminish the Internet's capability as a communications medium. As Secretary of State Hillary Clinton noted last year:

> [T]he new iconic infrastructure of our age is the internet. Instead of division, it stands for connection. But even as networks spread to nations around the globe, virtual walls are cropping up in place of visible walls. . . . Some countries have erected electronic barriers that prevent their people from accessing portions of the world's networks. They've expunged words, names, and phrases from search engine results. They have violated the privacy of citizens who engage in non-violent political speech. . . . With the spread of these restrictive practices, a new information curtain is descending across much of the world.[5]

It would be not just ironic, but tragic, were the United States to join the ranks of these repressive and restrictive regimes, erecting our own "virtual walls" to prevent people from accessing portions of the world's networks. Passage of these bills will compromise our ability to defend the principle of the single global Internet—the Internet that looks the same to, and allows free and unfettered communication between, users located in Boston, Bucharest, and

5. Hillary Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010), http://www.state.gov/secretary/rm/2010/01/135519.htm.

Buenos Aires, free of locally imposed censorship regimes. As such, it may represent the biggest threat to the Internet in its history.

Copyright and trademark infringement on the Internet is a very real problem, and reasonable proposals to augment the ample array of enforcement powers already at the disposal of IP rights holders and law enforcement officials may serve the public interest. But the power to break the Internet shouldn't be among them.