Legally Speaking
Can Online Piracy Be Stopped by Laws?

Considering the legal responsibilities of Internet intermediaries in the aftermath of the Stop Online Privacy Act controversy.

While on a scuba diving trip in the Seychelles Islands earlier this year, I found myself worrying about pirates. Real pirates, as in people who attack boats, take hostages, and sometimes kill their prey. This kind of piracy has become unfortunately common in that part of the world.

On board our ship were four former British special forces soldiers who served as security guards. They were armed with semiautomatic weapons and on patrol, 24/7, for the entire trip. The danger was not just hypothetical. The frigate berthed next to us as we boarded had 25 pirates in its brig.

Waking up every morning to the prospect of encountering real pirates added brio to our excursion. It also induced reflections on use of the word “piracy” to describe copyright infringements. Downloading music is really not in the same league as armed attacks on ships.

As we were cruising from Mahe to Aldabra, I expected to be far away from it all. But the ship got a daily fax of the main stories being published in the New York Times. Among them were stories about the controversy over the proposed legislation known as the Stop Online Piracy Act (SOPA). SOPA would have given the entertainment industry new legal tools to impede access to foreign “rogue” Web sites that host infringing content and to challenge U.S.-directed Web sites that the industry thought were either indifferent or acquiescent to storage of infringing materials.

For a time, it seemed virtually inevitable that SOPA would become law. Yet because strong opposition emerged from technology companies, computer security experts, civil liberties groups and members of the general public, SOPA has been put on hold. It is unlikely to be enacted in anything like its original form.

This column will explain the key features of SOPA, why the entertainment industry believed SOPA was necessary to combat online piracy, and why SOPA came to be perceived as so flawed that numerous sponsors withdrew their support from the bill.

Blocking Access to “Foreign Rogue Web Sites”
As introduced, SOPA would have empowered the Attorney General (AG) of
the U.S. to seek court orders requiring foreign Web sites to cease providing access to infringing copies of U.S. works. Because "rogue" Web sites seemed unlikely to obey a U.S. court order, SOPA further empowered the AG to serve these orders on U.S. Internet intermediaries who would have been required to take "technically feasible and reasonable measures" to block their users from accessing the foreign Web sites. This included "measures designed to prevent the domain name of the foreign infringing site...from resolving to that domain name's Internet protocol address." These measures need to be undertaken "as expeditiously as possible," but no later than five days after receipt of the orders.

Upon receiving a copy of a rogue Web site order, search engines would have been required to block access to the sites even if users were searching for items that would otherwise have brought the sites to their attention. Internet service providers would have had to ensure that users who typed certain URLs (for example, http://thepiratebay.se) into their browsers could not reach those sites. Payment providers (such as Visa or Mastercard) would have had to suspend services for completing transactions. Internet advertising services would have had to discontinue serving ads and providing or receiving funds for advertising at these sites.

Those who failed to comply with the DNS blocking obligations could expect the AG to sue them. The AG was also empowered to sue those who provided a service designed to circumvent this DNS blocking (for example, a plug-in or directory that mapped blocked URLs with numerical DNS representations).

Frustrated by the weak enforcement of intellectual property rights (IPRs) abroad, the U.S. entertainment industry urged Congress to adopt SOPA as the best way to impede online infringements. Foreign rogue Web sites might still be out there, but if U.S.-based Internet intermediaries blocked access to the sites, users would not be able to access infringing materials through U.S. intermediaries.

Because ISPs in the U.S. and abroad have no duty to monitor what users do on their sites, it is easy for sites to become hosts of large volumes of infringing materials. Some operators seemingly turn a blind eye to infringement, some encourage posting of infringing content, while other sites may just be misused by infringers. By cutting off sources of transactional and advertising revenues, the hope was to discourage these sites from continuing to operate.

**Challenging U.S.-Directed Web Sites**

SOPA would also have given holders of U.S. intellectual property rights (IPRs) power to challenge "U.S.-directed sites dedicated to the theft of U.S. property." At first blush, it might seem that reasonable persons should support a law crafted to target such sites. But "dedicated to the theft of U.S. property" was defined in a troublingly ambiguous and overbroad way. It included operators of sites that were taking "deliberate actions to avoid confirming a high probability of the use of [that] site to carry out acts" in violation of copyright or anti-circumvention rules. Also included was any site that was "primarily designed or operated for the purpose of, ha[d] only a limited use other than, or [was] marketed by its operator or another acting in concert with that operator in, offering goods or services in a manner that engages in, enables, or facilitates" violations of copyright or anti-circumvention laws.

SOPA would have enabled firms who believed themselves to be harmed by one of these sites to send letters to payment providers and/or to Internet advertising services to demand that they cease providing services to sites alleged to be "dedicated to the theft of U.S. property" shortly after receiving such letters.

Payment providers and Internet advertising services were then tasked with notifying the challenged sites about the "dedicated-to-theft" allegations against them. Challenged sites could contest these allegations by sending counter-notices to the payment providers and Internet advertising services. But without a counter-notice, payment providers and Internet advertising services had to cease further dealings with the challenged Web sites.

Content owners could also sue dedicated-to-theft sites directly to enjoin them from undertaking further actions that evidenced their dedication to theft. SOPA also authorized content owners to sue payment providers or advertising services who failed to comply with demands that they cease dealing with challenged Web sites.

**SOPA's Flaws**

The main problems with SOPA insofar as it would have employed DNS blocking to impede access to foreign rogue Web sites were, first, that it would undermine the security and stability of the Internet as a platform for communication and commerce and second, that it would be ineffective.

SOPA is fundamentally inconsistent with DNSSEC (DNS Security Extensions), a protocol developed to avoid abusive redirections of Internet traffic, whether by criminals, autocratic governments, or other wrongdoers. Computer security experts spent more than a decade developing DNSSEC, which is now being implemented all over the world, including by U.S. government agencies.

As the USACM Public Policy Committee observed in a letter sent to members of Congress, DNSSEC Web site operators cannot reliably block offending sites "and so may be faced with the choice of abandoning DNSSEC or being in violation of issued court orders."

This letter explained why DNS blocking would be ineffective. "[It is effectively impossible to bar access to alternate DNS servers around the globe because there are millions of them on the Internet. Use of those servers "allows for bypassing of DNS blocking." Circumvention of DNS blocking is, moreover, "technically simple and uni-

---

**The safe harbors have been an important factor in the extraordinary growth of the Internet economy.**
versally available." Browser add-ons to avoid DNS blocking have already been developed and would be available on servers outside the U.S., even if illegal in the U.S.

The main problems with the dedicated-to-theft provisions of SOPA were, first, that it was too imprecise and second, that it represented a dramatic change in the rules of the road affecting Internet intermediaries.

What does it mean, for instance, for an Internet intermediary to take "deliberate actions to avoid confirming a high probability" of infringement on the site? If Viacom tells YouTube it has found infringing clips of "South Park" shows on its site, does YouTube become a site dedicated to the theft of Viacom's property if it does not investigate these claims? If Universal Music Group objects to the resale of MP3 files of its music on eBay, does eBay become a site dedicated to theft of Universal's property because one or more of its users offer the MP3 files for sale there?

Many Internet companies considered the dedicated-to-theft definition to be fundamentally inconsistent with the safe harbors established by the Digital Millennium Copyright Act (DMCA). Under the DMCA, Internet intermediaries are obliged to take down infringing materials after they are notified about specific infringements at specific parts of their Web sites. They have no obligation to monitor their sites for infringement. The safe havens have been an important factor in the extraordinary growth of the Internet economy.

It may be apt to characterize sites such as Napster, Aimster, and Grokster as having been dedicated to the theft of U.S. intellectual property, but existing copyright law supplied copyright owners with ample tools with which to shut down those sites.

Had the entertainment industry sought more narrowly targeted rules aimed at inducing payment providers and Internet advertising services to stop the flow of funds to sites that were really dedicated to infringement, such a law might have passed. But that was not SOPA.

Conclusion
The collapse of support for SOPA was principally due to concerted efforts by Internet service providers (including Wikipedia, which went "dark" one day to protest SOPA), computer security experts, civil society groups, and millions of Internet users who contacted their Congressional representatives to voice opposition to the bill.

Because SOPA was a flawed piece of legislation, the collapse was a good thing. It would, however, be a mistake to think the battle over Internet intermediary liability for infringing acts of users has been won for good.

The entertainment industry is almost certainly going to make further efforts to place greater legal responsibilities on Internet intermediaries. This industry believes intermediaries are the only actors in the Internet ecosystem who can actually affect the level of online infringements that contributes to entertainment industry panics.

An odd thing about the entertainment industry is its deeply skewed views about piracy. In movies such as Pirates of the Caribbean, the industry glamorizes brigands who attack ships by depicting them as romantic heroes who have great adventures and engage in swashbuckling fun. Yet, it demonizes fans who download music and movies as pernicious evildoers who are, in its view, destroying this vital part of the U.S. economy. Something is amiss here, and it is contributing to a profound disconnect in perspectives about how much the law can do to bring about changes in norms about copyright.

Pamela Samuelson (pam@law.berkeley.edu) is the Richard M. Sherman Distinguished Professor of Law and Information at the University of California, Berkeley.

Calendar of Events
July 15–16
Extreme Scaling Workshop,
Chicago, IL
Contact: Bill Kramer,
Email: kramer@illinois.edu

July 15–19
26th ACM/IEEE/SCS Workshop on Principles of Advanced and Distributed Simulation, Zhangjiang, China,
Sponsored: SIGSIM,
Contact: Jason Liu,
Email: liux@cis.fiu.edu

July 15–20
International Symposium on Software Testing and Analysis,
Minneapolis, MN,
Sponsored: SIGSOFT,
Contact: Mats Heimdahl,
Email: heimdahl@es.msu.edu

July 16–18
ACM Symposium on Principles of Distributed Computing,
Funchal, Portugal,
Sponsored: SIGOPS,
Contact: Dariusz Kowalski,
Email: darek@lix.ia.uzh.ch

July 16–20
the 6th ACM International Conference on Distributed Event-based System,
Berlin, Germany,
Sponsored: SIGSOFT,
Contact: Francois Bry,
Email: bry@lmu.de

July 16–20
User Modeling, Adaptation and Personalization,
Montreal, Canada,
Contact: Nkambou Roger,
Email: nkambou.roger@uqam.ca

July 22–25
International Symposium on Symbolic and Algebraic Computation,
Grenoble, France,
Contact: Joris van der Hoeven,
Email: vdhoeven@lix.polytechnique.fr

July 24–27
International Conference on e-Business,
Rome, Italy,
Contact: Prof. Mohammad S. Obaidat,
Email: obaidat@monmouth.edu