EDUCAUSE

Higher Education Concerns About the Stop Online Piracy Act ("SOPA"), with Initial Suggestions for Addressing Them

The "Stop Online Piracy Act" or "SOPA" (H.R. 3261) is the House version of S. 968, the Senate's "PROTECT IP Act" or "PIPA." These notes, summarized by EDUCAUSE, draw on extensive discussions among a broad array of colleges, universities, and higher education associations.

As both large-scale users and producers of intellectual property, higher education institutions support the goal of balanced copyright laws. Unimpeded copyright infringement undermines core educational values. We have long advocated that copyright infringement be addressed by targeting how infringers advertise their wares and secure their revenues, and we believe that much of what is proposed in SOPA responds appropriately to copyright infringement in this way.

The higher education community believes that websites whose main purpose and activity is to enable and promote infringement should be targeted aggressively by the content owners in whose interest it is to bring civil actions. In cases of commercial-scale infringement, such websites should be targeted by law enforcement. Unfortunately, although its goals are appropriate, SOPA goes beyond these reasonable, pragmatic mechanisms for addressing infringement by casting its net more widely. This overbroad response not only incorporates problems previously identified with the PROTECT IP Act, it makes those worse and creates further problems.

SOPA introduces sweeping new risks for and imposes new responsibilities on mainstream websites offering legitimate online services, including those hosted by colleges and universities. It gives rights holders private rights of action to employ against any legitimate as well as illegitimate online services, foreign or domestic. These can expose institutions of higher education—and any other organization or company that sponsors a broad array of separately-managed websites—to harassment, to unwarranted and expensive litigation, and to new forms of liability. In short, in the name of stopping infringement, SOPA can also inhibit or stop a far wider range of perfectly legitimate activity.

Separately, SOPA includes a narrow requirement that unfortunately has major implications: requiring that under some circumstances the Domain Name System—"DNS", the Internet's "phonebook"—be modified. The DNS provision has generated heated discussion and controversy. It would be unfortunate if the relatively minor DNS and anti-circumvention provisions in the bill were to divert attention from its valuable, proper, and principal focus on mechanisms that directly and appropriately target those who advertise or collect revenues for copyright infringers. If there are problems with how the Internet's core architecture works, the productive way to address these is through well-established, effective global mechanisms such as the Internet Engineering Task Force, rather than through legislation. We strongly suggest that the DNS provisions be removed from the bill, and that discussion of such countermeasures be moved to a more appropriate forum.

We urge that these issues be addressed and be revised substantially before H.R. 3261 proceeds any further.

Four main aspects of H.R. 3261 are problematic for higher education:

1. **Broad Definitions Create Uncertainty for Colleges, Universities, and Their ISPs**

    a. The bill's definitions of infringing websites are vague and overly broad. Unlike PIPA, SOPA's definition of sites "dedicated to the theft of U.S. property" includes not just sites that are dedicated to or even primarily focused on infringement, which is a clear, comprehensible, and appropriate definition, but rather appears to extend the definition to any site that "enables or facilitates" infringement (Section 103(a)(1)(B)(i)). This language could sweep in virtually any multi-use technology, contrary to the Supreme Court's holding in *Sony v. Betamax* (464 U.S. 417 (1984)).

2. **New Monitoring Mandates Contravene the DMCA Safe Harbor Provisions**

   a. SOPA adds a new obligation that ISPs not "avoid confirming" infringement (Section 103(a)(1)(B)(ii)(I)). This likely would induce ISPs worried about potential liability to actively monitor and perhaps interfere with their users' activities—the double negative is easily read, in today's litigious world, as a positive requirement to "confirm" that users are not violating copyrights. This is precisely the type of monitoring that the Digital Millennium Copyright Act ("DMCA", Pub. L. 105-204) was meant to prevent. SOPA would upset the balance of the DMCA by shifting the burden of copyright enforcement to innocent intermediaries, including higher education institutions, and it would subject users to pervasive monitoring of their activities online.

   b. As currently drafted, SOPA would classify as "dedicated to the theft of U.S. property" Internet services that the DMCA was expressly designed to shield, i.e., services with legitimate uses that could nevertheless be abused by some users. Use of "enables or facilitates" in Section 103(a)(1)(B)(i) creates this ambiguity.

3. **Felony Streaming Provision Creates New Liability for Good Faith, Non-Profit Users**

   a. Unlike S. 968, SOPA would apply felony penalties to non-commercial actors such as colleges and universities (Section 201(a)(1)), even though these entities play no intentional role in infringement. Through the "should have known" language in Section 201(a)(1)(C), SOPA also expands "willful infringement" to include good-faith actors. The Library Copyright Alliance letter of 8 Nov 2011 on streaming provides excellent analysis on this point (see http://www.librarycopyrightalliance.org/bm~doc/lca-sopa-8nov11.pdf), and the concerns raised there apply equally well to higher education.

4. **Domain Name System (DNS) Filtering and Redirection Set a Bad Precedent, and Will Not Work**

   a. The filtering mandate (Section 102(c)(2)(A)(iv)) and the anti-circumvention ban (Section 102(c)(4)(A)(ii), Section 102(c)(4)(D)) in SOPA would impose major new costs and risks on those providing non-infringing online communication within the U.S., thereby undercutting the competitive advantage the U.S. currently enjoys in network-based services, technologies, and innovation.

   b. SOPA requires that in some cases the hostnames or subdomains for offending sites be redirected to a different site (Section 102(c)(2)(A)(i)). Redirection of the sort embodied in SOPA would be contrary to well-established principles and security measures designed to foil cybercriminals, one of whose preferred techniques is DNS redirection.

   c. SOPA allows the government to obtain injunctions against anti-censorship software that circumvents the government's DNS-blocking efforts (Section 102(c)(4)(A)(ii), Section 102(c)(4)(D)). Such technology mandates are inevitably too broad, as has become clear in earlier technology-suppression efforts, and they undermine important free speech values.

   d. In many cases, DNS resolution is by DNS servers that organizations run for their own internal purposes, rather than authoritative servers run by ISPs or domain managers. Section 102 appears to impose requirements on *non-authoritative* DNS servers, even though these are numerous and not easy to find—they are in every wireless hotspot or coffee shop, and indeed Congress itself likely operates its own. We believe that it will be neither practical nor desirable to target every non-authoritative DNS server, and so DNS filtering simply cannot be very effective (see http://www.redbarn.org/files_redbarn/PROTECT-IP-Technical-Whitepaper-Final.pdf).

Some changes that would reduce or eliminate these problems:

1. Use a narrower, pragmatic definition of offending websites, focusing on the sites that actually provide offending content rather than ISPs and network operators that provide access to them, however inadvertently. As one of many examples, albeit a very important one, remove the text "enables or facilitates" from Section 103(a)(1)(B)(i).

2. On the grounds that they would be ineffective and facilitate abuse, eliminate all of the DNS provisions. In Section 102(c)(2)(A)(i), for example, this could be achieved by eliminating the text "including measures designed to prevent the domain name of the foreign infringing site (or portion thereof) from resolving to that domain name’s Internet Protocol address". Text referring to DNS elsewhere in SOPA would also need to be removed.

3. Clarify through explicit language that any entity whose policies and actions qualify it for the DMCA safe harbor, as defined in that Act, is not an infringing site liable under SOPA.

4. In Section 201(c), strike "good faith reasonable basis in law to believe" from the first sentence and replace it with "good faith belief." This removes the negative implication that a good faith actor could nevertheless be a willful infringer, which is inconsistent with the majority interpretations of "willful" copyright infringement in existing case law. (See, e.g., U.S. v. Moran, 757 F. Supp. 1046 (D. Neb. 1991)). To further clarify the standard, the rule of construction in 201(c) could be amended to add, as the second sentence, the following language, based on Moran: "Rather, for purposes of the amendments made in this section, willfulness should be interpreted to mean a voluntary, intentional violation of a known legal duty." The remainder of 201(c) would remain unchanged.

11/22/11h