Markham C. Erickson
Partner, Holch & Erickson LLP and
Executive Director, NetCoalition

H.R. 3261, "Stop Online Piracy Act" ("SOPA")
Explanation of Bill and Summary of Concerns[1]

SOPA was introduced on October 26, 2011 by Chairman Lamar Smith (R-TX) of the House Committee on the Judiciary. The original co-sponsors are Representatives Conyers (D-MI), Goodlatte (R-VA), Deutch (D-FL), Chabot (R-OH), Ross (R-FL), Blackburn (R-TN), Bono Mack (R-CA), Terry (R-NE), Schiff (D-CA).

Contents of This Paper.

I. Introduction.

SOPA is an 80-page Internet regulatory proposal that goes well beyond what supporters originally sought from Congress: finding a way to target the "worst-of-the-worst" offshore sites that peddle illegal goods to U.S. consumers by operating outside of the Department of Justice's jurisdiction.

II. Highlights of What the Legislation Does.

Sec. 101.

- Includes 24 definitions, including many new definitions for developing Internet technologies.

[1] This draft only covers Title I, Sections 101-104. Analysis of Title II is forthcoming.

Sec. 102.

- Authorizes the Attorney General to sue a "foreign infringing site" with new definition of what constitutes a "foreign infringing site."

- Includes a new "in rem" jurisdictional theory to provide U.S. courts with jurisdiction over foreign sites that are, among other things, available to users in the United States.

- If successful, the Attorney General can serve a copy of the court's order on Internet service providers, Internet search engines, Internet advertising services and payment network providers. These entities would be required within five days to take technically feasible and reasonable measures to block access to or cease financial and advertising transactions with the foreign infringing site.

Sec. 103.

- Establishes a private right of action that authorizes plaintiffs to seek remedies against both domestic and foreign websites that are "dedicated to the theft of U.S. property."

- Plaintiff can be anyone with an intellectual property right harmed by copyright or trademark infringement on the site (the plaintiff need not own the infringed copyright or trademark).

- Under a notice-and-terminate process, plaintiff notifies payment network provider or Internet advertising service to cease servicing an allegedly illegal site. The advertising service or payment network provider must take action within five days.

- Requires the Internet advertising service or payment network provider to "timely" notify allegedly illegal site of the notice.

- Allows the allegedly illegal site to send a counter-notice to the advertising service or payment network provider (but does not require the advertising service or payment network provider to restore service).

- If the advertising service of the payment system provider complies with the counter-notice, the plaintiff can sue the operator of a U.S. website under normal jurisdictional principles or a foreign site under a new "in rem" theory of jurisdiction. If the court finds that the site is "dedicated to the theft of U.S. property" as defined under the statute, the court can issue injunctive relief. Additionally, the court can issue an order that the plaintiff can then serve on advertising services and payment system providers. The advertising service or payment network provider must take technically feasible and reasonable measures to terminate service to the site within five days of receiving the order.

- Plaintiff can initiate a "show cause" proceeding against the payment network provider or Internet advertising service the plaintiff believes the payment network provider or Internet advertising service has not complied with its obligation to terminate service. The burden is on the payment network provider or advertising service to defend its action (or inaction) under the threat of monetary sanctions.

- Payment network providers and advertising services are given immunity from future, collateral lawsuits stemming from action taken to comply with an order under this section.

Sec. 104.

- Provides immunity to a service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name registrar for voluntarily terminating services, blocking financial transactions, or blocking access to an Internet site with which the entity "reasonably" believes is a "foreign infringing site" or a site "dedicated to theft of U.S. property," so long as the entity "reasonably" believes the action is consistent with the entity's terms of service or other contractual rights.

III. Concerns with SOPA.

- **Effectively Overturns Current Law.** SOPA threatens the ongoing success of the ***U.S. Internet industry, which is one of the most successful and fastest growing sectors of the national economy***, by imposing regulations and liabilities on Internet companies that merely serve as conduits for someone else's communication. This is a ***direct reversal of the federal laws and policies – most significantly the Digital Millennium Copyright Act ("DMCA") – that have allowed the Internet economy to grow and succeed.***

- **Subjects U.S. Firms to Three New Statutory Standards of Infringement**. SOPA creates new, vague theories of secondary liability that expose lawful, U.S. Internet firms, cloud computing services, and social networks to ***new litigation***.

- **Eliminates Business Certainty for U.S. Internet Firms**. SOPA introduces a confusing patchwork of regulations ***where a site that has certainty that it will not be subject to liability under the DMCA can nonetheless be deemed an illegal site under SOPA***.

- **Technology Mandates**. SOPA exposes U.S. Internet companies and payment network providers to ***technology mandates***, where federal judges can impose or second-guess technological measures used to block access or service to Internet sites at the request of law enforcement or private parties.

- **Creates a New Private Right of Action Against Lawful U.S. Companies**. SOPA provides ***a private right of action against sites in the U.S. that have violated no existing law and against lawful payment network providers and Internet advertising services***.

- **Exposes lawful U.S. firms to liability without due process.** SOPA encourages firms to shut down, block access to, and stop servicing U.S. and foreign websites that copyright and trademark owners allege are illegal ***without any due process*** or ability of a wrongfully targeted website to seek restitution.

- **Threatens Critical U.S. Infrastructure**. SOPA proposes technological solutions to block access to unlawful sites that ***will not work and instead create security risks to critical U.S. infrastructure***.

- **Chills Free Speech.** SOPA grants new powers to both law enforcement and private actors to filter the Internet and block access to tools to get around those filters, inadvertently giving support to similar efforts by oppressive, undemocratic regimes in other countries.

IV. Details of and Support for Concerns.

1. Effectively Overturns Current Law. SOPA threatens the ongoing success of the ***U.S. Internet industry, which is one of the most successful and fastest growing sectors of the national economy***, by imposing regulations and liabilities on Internet companies that merely serve as conduits for someone else's communication. This is a ***direct reversal of the federal laws and policies – most significantly the Digital Millennium Copyright Act ("DMCA") – that have allowed the Internet economy to grow and succeed.***

- The DMCA, which was passed by Congress at the beginning of the commercial Internet, is a critical part of the legal foundation that has made the U.S. Internet industry the most successful in the world. The policy decision reflected in that statute is that Internet companies should not have to affirmatively police their users' activities or be liable for the content or conduct of third parties who use their platforms.

- Under federal law, parties that use the phone lines to engage in illegal activity pose no threat of liability to telephone companies because the companies are merely conduits. In the Internet space, under the DMCA, an Internet company that serves as a conduit for third party communications receives a safe harbor from liability if it creates a process to respond to a copyright owner's notice about infringing content on the Internet company's platform.[2]

[2] 17 U.S.C. § 512(a),(c).

- The DMCA carefully balances the competing interests of different stakeholders. It protects end users by making clear that Internet companies do not need to monitor their users' activities in order to qualify for the safe harbor. It protects copyright owners by providing them a quick and efficient means of removing infringing content from the Internet by notifying Internet companies. It protects website operators and others posting content on the Internet by targeting the relief at the infringing content and by providing a mechanism for counter-notification.

- SOPA circumvents this careful balance. Its sweeping definition of a website "dedicated to theft of U.S. property" would include virtually any website that hosts or links to third party content. SOPA would allow extraordinary remedies against such websites, including the termination of financial resources in the form of ad revenue or payment for transactions. The possibility of termination would force Internet companies to take a completely different approach to hosting and linking to third parties content. The threat of being shut down and lack of clarity about what actions are required by SOPA will significantly deter current and future Internet businesses from investing in new ventures. The Internet would become less innovative, entrepreneurial and diverse.

- The problem begins with the sweeping definition of a website "dedicated to theft of U.S. property" in section 103(a). Under this definition, a site is "*dedicated to the theft of U.S. property"* if even a portion of it "enables or facilitates" someone else's infringement, whether or not such activity meets the requirements for secondary liability under existing law.[3] Secondary liability in copyright and trademark are nuanced judge-made doctrines that balance competing interests. The SOPA definition lacks this nuance and balance. Moreover, because under existing law there is no secondary liability for violations of section 1201 (which already prohibits "trafficking" in tools that circumvent content protection technologies), the bill creates new obligations on sites that are not violating that law.

- A site can also be declared to be "dedicated to theft of U.S. property" if it takes "deliberate actions to avoid confirming a high probability" that the site has been used for infringing activities. This is true whether or not the "failure to act" would itself violate existing law. And because rightsholders will say that there is a "high probability" that social networking and user-generated content sites are used for infringement by some users, this provision would effectively force those site operators to actively monitor their users' activities. This is flatly inconsistent with the DMCA's provision stating that service providers do *not* have to monitor user activities.

- Similarly, if *any* "portion" of the site "promoted" the infringement of *any* content, it would meet the definition. For example, a blogging site, which contains millions of pages of blogs from hundreds of thousands of users, could be targeted as a "site dedicated to the theft of U.S. property" if one page or one blog on the service contains or promotes infringing content. A social networking site would be a site "dedicated to the theft of

[3] *Id.* at Section 103(a)(2) [Page 25, line 4].

U.S. property" if one user's page contains infringing content. An e-commerce site would be a site "dedicated to the theft of U.S. property" if only one merchant's page sells counterfeit goods. A cloud computing service with millions of users is "dedicated to the theft of U.S. property" if one user engages in or promotes infringing conduct.

- Significantly, even if an Internet company complies with all of the requirements for the DMCA safe harbor provisions (including notice-and-takedown and terminating repeat infringers), it still could fall within the definition of a site dedicated to the theft of U.S. property. Plaintiffs will argue that compliance with the DMCA safe harbors merely limits remedies, but does not provide an affirmative defense to infringement claims. Therefore, plaintiffs will argue, a site can be completely compliant with the DMCA, and still satisfy the definition of "site dedicated to theft."

- SOPA then imposes drastic and disproportionate remedies on sites that allegedly meet the definition of site dedicated to theft of U.S. property -- without any judicial finding. Upon receiving a notice from a rightsholder that a particular website is dedicated to the theft of U.S. property, an advertising service or payment network provider is required to stop servicing the Internet company site within five days. There is the opportunity for the Internet company to submit a counter-notice, but the time line is so compressed that the site could be cutoff before it has the opportunity to respond. And, thanks to the broad immunity provisions in the bill, the advertising service or payment network provider has no obligation to restore service once it receives a counter-notice.

- Assuming that the Internet company does file a counter-notification, and the advertising service or payment system provider respects the counter-notification, the rightsholder can then go to court seeking an order declaring the Internet company site a site dedicated to the theft of U.S. property. Because of the breadth of the definition, as describe above, a broad array of U.S. sites that fully comply with U.S. law could find themselves declared to be "dedicated to the theft of U.S. property." The rights holder would then serve the order on the advertising service or payment network provider, which would be required to terminate service.

- In sum, while the DMCA targets the specific infringing content and specific repeat infringers, SOPA instead targets an entire website even if only a small portion hosts or links to some infringing content. Although its supporters claim that SOPA is directed to "foreign rogue websites," the definition of "website dedicated to theft of U.S. property" is not limited to foreign sites, or to the worst of the worst. Rather, companies that comply with the DMCA would be subject to SOPA's remedies. Similarly, sites that have not violated any copyright or trademark laws could be targets for "enabling or facilitating" some third party's misdeeds.

2. Eliminates Business Certainty for U.S. Internet Firms. SOPA introduces a confusing patchwork of regulations ***where a site that has certainty that it will not be subject to liability under the DMCA can nonetheless be deemed an illegal site under SOPA***.

- Current law promotes an "innovation without having to ask permission" environment that has made the U.S. Internet sector the most successful technology sector in the world. This is due in no small part because of the balanced legal framework Congress created at the start of the commercial Internet.

- Venture capitalists and other investors know that they will have certainty that a website that allows user-generated content will not be in legal jeopardy as long as it satisfies the safe harbor conditions in the DMCA. Unfortunately, a site that enjoys the DMCA safe harbor could nonetheless be targeted by termination notices and held liable under SOPA. That is because the new liabilities created by SOPA do not have an exception that protects lawful U.S. sites that are compliant with the DMCA's notice-and-takedown requirements.

3. Technology Mandates. SOPA exposes U.S. Internet companies and financial services firms to ***technology mandates***, where federal judges can impose or second-guess technological measures used to block access to Internet sites at the request of law enforcement or private parties.

- Under section 102, a service provider (which under the bill ranges from big telephone and cable companies to university networks, libraries, and private businesses[4]) is required to take "technically feasible and reasonable measures designed to prevent access" to illegal sites, *including, but not limited to*[5] measures designed to prevent that domain name of the infringing site from resolving to that domain name's Internet Protocol address.[6] Because the service provider domain name remedy is not the exclusive remedy, the Attorney General and a judge can require a service provider to create other technology solutions to block access to illegal sites. What else might be required beyond these steps is not specified.

- The bill's caveat that a service provider does not have to "modify its network, software, systems, or facilities" is contradicted by the words "other than as directed under this subparagraph," which immediately proceeds the caveat.[7]

- An Internet "search engine"[8] is required to take "technically feasible and reasonable measures" to prevent an illegal site from being served as a direct hypertext link.[9]

---

[4] In SOPA, the definition of "service provider" means, among other things, providers of Internet access and transport for Internet communications or any "provider of online services" that operate a "nonauthoritative domain name system servicer." H.R. 3261 Section 101(22) (cross-referencing 17 U.S.C. Section 512(k)). Providers of Internet access that operate nonauthoritative domain name services include university systems, libraries, and private businesses.

[5] H.R. 3261, Section 101(22) [Page 4, lines 20-21] (emphasis added).

[6] H.R. 3261, Section 102(c)(2)(A)(i) [Page 13, lines 21-25 through Page 14, lines 1-6].

[7] *Id.* at 102(c)(2)(A)(ii)(I) [Page 14, lines 13-15].

[8] The definition of Internet search engine under SOPA is not clear and arguably includes any site with a "search box" that allows users to search for content elsewhere on the site or domain. ("The term 'Internet search engine' means a service made available via the Internet that searches…information or Web sites *available elsewhere* on the Internet." H.R. 3261 at 101(16) [Page 6, lines 12-16] (emphasis added).

Curiously, this provision does not include the service provider limitation that it does not have to modify its network.

- Payment network providers are required to take "technically feasible and reasonable measures" to prevent its service from completing payments to an illegal site.[10]

- Internet advertising services are required to take "technically feasible and reasonable measures" to prevent its service from completing payments to an illegal site.[11]

- Section 102 allows the Attorney General to ask a court to second-guess whether these four categories of service providers have taken technically feasible and reasonable measures, thereby inviting the court to mandate further measures. Moreover, under section 103, a private plaintiff can ask the court to impose additional technology mandates on payment processors and ad networks.

4. Exposes U.S. Payment Network Providers and Internet Advertising Systems to Private Legal Actions

- Under Section 103, if a private "qualifying plaintiff" believes that a payment network provider or an advertising service has not complied with its obligations under SOPA, the private plaintiff can initiate a "show cause" proceeding against the payment network provider or advertising service. In addition to requiring the provider or service to take the additional technical measures described above, the court can impose monetary sanctions.

- The only affirmative defense specified in connection to the "show cause" proceeding is that the payment network provider or advertising service does not have "the technical means to comply with this subsection without incurring an unreasonable economic burden," a highly ambiguous standard. A payment system provider or advertising service would presumably be required to provide expert testimony, subject to cross-examination, to establish that it had met its burden.

- The "qualifying plaintiff" entitled to initiate the section 103 process is not limited to the owner of a copyright or trademark infringed by or through a site "dedicated to the theft of U.S. property." Instead, the term "qualifying plaintiff" means any holder of an intellectual property right "harmed" by the activities that cause the website to fall within the definition of a site dedicated to theft of U.S. property, even if the plaintiff does not own the trademark or copyright infringed on the site.[12] Thus, the owner of a copyright, patent, or trade secret that suffers economic harm by virtue of the free availability of a competitor's product on a site "dedicated to theft of U.S. property" could initiate the section 103 process, even though the competitor has decided not to enforce its rights.

---

[9] *Id.* at 102(c)(2)(B) [Page 15, lines 11-20].
[10] *Id.* at 102(c)(2)(C) [Page 16, lines 22-24], 103(b)(1) [Page 27, lines 1-12].
[11] *Id.* at 102(c)(2)(D) [Page 17, lines 5-6], 103(b)(2) [Page 27, lines 13-24]..
[12] Section 103(a)(2) [Page 26, lines 18-23].

5. Exposes lawful U.S. firms to liability without due process. SOPA encourages firms to shut down, block access to, and stop servicing U.S. and foreign websites that copyright and trademark owners allege are illegal ***without any due process*** or ability of a wrongfully targeted website to seek restitution.

- Section 104 of SOPA puts the property rights of U.S. websites at jeopardy, without any due process, by providing complete immunity for a service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name registrar for voluntarily blocking access to or ending financial affiliation with an Internet site so long as there is a "reasonable" belief that the site is a site "dedicated to theft of U.S. property."[13]

- If a website's property, business, or reputation has been wrongfully harmed by an entity taking action against the website pursuant to Section 104, there is no mechanism for the wronged website to seek restitution.

- Under this provision, a rightsholder can pressure a service provider to censor a site or terminate its relationship with a site that the rightsholder claims is "dedicated to the theft of U.S. property" by threatening to sue the service provider with a claim of contributory infringement if it does not shut down the accused website. Faced with this potential lawsuit, and provided with the section 104 immunity, the service provider will have a strong incentive to shut down the accused website. In other words, the legislation systematically favors a copyright owner's intellectual property rights and strips the owners of accused websites of their rights.

[13] *Id.* at 104 [Page 47, lines 11-25 through Page 48, lines 1-5].

6. Proposes "Technological" Solutions to Block Access to Unlawful Sites, which Will Not Work and Instead Create Security Risks to Critical U.S. Infrastructure.

- SOPA requires an Internet service provider to take "technically feasible and reasonable measures designed to prevent access by its subscribers…to the foreign infringing site…, including measures designed to prevent the domain name of the …site…from resolving to the domain name's Internet Protocol address."[14]

- Leading Internet security engineers agree that the proposed measure to block the domain name from resolving to the Internet Protocol address ("DNS remedy") will not work because it—

    - is easily circumvented by the user or targeted website;

    - thwarts a10-year effort to impose new security protocols in the DNS system, called DNS-Sec, which is designed to prevent an ISP (or anyone else) from interfering with a secure connection between the user and a desired website. This security system was implemented to make sure that when a user seeks to go to wellsfargo.com, the user can be assured that he or she will go to the authenticated Wells Fargo website; and

    - introduces malware to critical infrastructure as users inevitably turn to offshore, untrustworthy DNS providers as an alternative to the censored DNS services offered by their ISPs. Like any virus, once introduced to the network, the malware will spread.

7. **Authorizes Government Censorship of the Internet.** SOPA grants new powers to both law enforcement and private actors to filter the Internet and block access to tools to get around those filters, giving support to similar efforts by oppressive, undemocratic regimes in other countries.

- The proposed DNS technological remedy is not only ineffective and risky to critical infrastructure; it runs contrary to the US government's commitment to advancing a single, global Internet and free flow of information across it. Its inclusion risks setting a precedent for other countries, to use DNS mechanisms to enforce a range of domestic policies, erecting barriers on the global medium of the Internet. Non-democratic regimes could seize on the precedent to justify measures that would hinder online freedom of expression and association.

- Similarly, the bill institutes government-mandated censorship of Internet search results. For years, search engines have been pushing back against non-democratic regimes that have sought to limit the universe of information retrieved through Internet searches. SOPA sets an alarming precedent that undercuts the resistance to the actions of those regimes.

[14] Section 102(c)(2)(A) (Page 13, lines 20-25 though Page 14, lines 1-10].

- To date, Congress has not determined what behavior would establish a U.S. court's jurisdiction over a foreign website. SOPA's provides that a foreign site is subject to jurisdiction if, among other things, it "does not contain reasonable measures to prevent such goods and services from being obtained in or delivered to the United States."[15] Foreign regimes have sued U.S. Internet companies because content or goods on their platforms are being sought after by the foreign regime's citizens, and the Internet company has not taken affirmative measures to block such access. If Congress enacts SOPA, other countries will be emboldened to claim jurisdiction over U.S. Internet firms for activities that are not directed at the foreign country's citizens and which are lawful in the United States.

[15] H.R. 3261, at Section 101(23)(C).