

*Before the*  
House Judiciary Committee  
*Regarding*  
H.R. 3261, the “Stop Online Piracy Act”  
November 16, 2011  
**Statement of Edward J. Black**  
President and CEO, Computer & Communications Industry Association

---

On behalf of the Computer & Communications Industry Association, I offer for the committee’s consideration this statement on the subject of H.R. 3261, the “Stop Online Piracy Act.” (SOPA). The Computer & Communications Industry Association (CCIA) joins with the many prominent technology entrepreneurs, CEOs and executives who have expressed serious concerns about the regulatory strategy proposed in SOPA and its Senate counterpart, the PROTECT-IP Act.<sup>1</sup> These concerns have been also echoed by more than 50 prominent venture capitalists,<sup>2</sup> prominent Internet engineers,<sup>3</sup> libraries,<sup>4</sup> and over 100 law professors,<sup>5</sup> uniting constituencies as diverse as Demand Progress and the Tea Party Patriots.<sup>6</sup> Just yesterday, AOL, eBay, Facebook, Google, LinkedIn, Mozilla, Twitter, Yahoo!, and Zynga Game Network wrote this committee in opposition to this misguided legislation.<sup>7</sup> Concerns have also been voiced by numerous organizations, including our industry colleagues, such as the Consumer Electronics Association, TechAmerica, and NetCoalition, as well as numerous NGOs, including the American Center for Law & Justice, the American Civil Liberties Union, the Brookings Institution, the Competitive Enterprise Institute,

---

<sup>1</sup> See Letter from 130 entrepreneurs, founders, CEOs and executives to U.S. Congress, Sept. 8, 2011, available at <http://opinion.latimes.com/files/entrepreneurs-worried-about-pipa.pdf>.

<sup>2</sup> See Letter from 53 venture capitalists to U.S. Congress, June 23, 2011, available at <http://http://bit.ly/NetVCPipaLetter>.

<sup>3</sup> See Internet Engineers’ Letter Urging Amendment of the PROTECT-IP Act, Oct. 12, 2011, available at <http://dak42.icann.org/meetings/dakar2011/presentation-protect-ip-amendment-letter-12oct11-en.pdf>.

See also Steve Crocker, et al., Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill, May 2011, available at <http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf>.

<sup>4</sup> See Letter from Library Copyright Alliance to Reps. Smith & Conyers, Nov. 8, 2011, available at <http://www.librarycopyrightalliance.org/bm~doc/lca-sopa-8nov11.pdf>.

<sup>5</sup> See Letter from 108 Law Professors in Opposition, July 5, 2011, available at <http://blogs.law.stanford.edu/newsfeed/files/2011/07/PROTECT-IP-letter-final.pdf>.

<sup>6</sup> Gautham Nagesh, “House members unveil Stop Online Piracy Act,” Oct. 26, 2011, <http://thehill.com/blogs/hillicon-valley/technology/189999-house-members-unveil-stop-online-piracy-act>.

<sup>7</sup> Company Letter in Opposition to SOPA and PROTECTIP, Nov. 15, 2011, available at <http://www.protectinnovation.com/downloads/letter.pdf>.

Computer Professionals for Social Responsibility, the Electronic Frontier Foundation, Free Press, Freedom House, the Future of Music Coalition, Human Rights Watch, the Institute for Intellectual Property & Social Justice at Howard University, the New American Foundation, Public Knowledge, the Save Hosting Coalition, the Sports Fans Coalition, and numerous others.<sup>8</sup> *None* of these organizations are testifying here today.

## **Summary**

In a time of economic distress, the Internet is one of the few bright spots in the U.S. economy. According to the National Economic Council, it adds \$2 *trillion* to U.S. GDP.<sup>9</sup> The Internet has had an unprecedented positive effect on the economic growth and prosperity in our world, and yet, according to McKinsey, the “magnitude of this transformation is still underappreciated. The Internet accounted for 21 percent of the GDP growth in mature economies over the past 5 years.”<sup>10</sup> It is antithetical to the political and economic interests of the United States to regulate the Internet. As recent events have demonstrated, authoritarian governments resent the openness and democratic nature of the Internet, and seek any cause to regulate it. Even democratic governments occasionally feel this temptation, and the United States cannot resist the regulation and repression elsewhere if we yield to pressure to do the same here.

Under certain circumstances, however, the extreme of Internet regulation may be the least bad option. In the case of SOPA, however, the regulatory framework needs significant revision.

### **I. Domain Name Blocking Threatens Internet Security.**

SOPA’s central approach is the blocking or filtering of domain names. Since the strategy of domain-based filtering was first proposed in Congress, Internet security experts have strongly advised against it. A recent white paper authored by prominent Internet engineers including Dan Kaminsky, the famous security researcher credited with “saving the Internet”<sup>11</sup> from critical DNS security bugs, explained that “[r]edirecting users to a resource that does not match what they

---

<sup>8</sup> See Center for Democracy & Technology, “Growing Chorus of Opposition to ‘Stop Online Piracy Act’”, Nov. 15, 2011 <<http://cdt.org/report/growing-chorus-opposition-stop-online-piracy-act>>.

<sup>9</sup> This yields over \$6,500 per person. Exec. Ofc. of the President, Nat’l Econ. Council/OSTP, *A Strategy for American Innovation: Driving Towards Sustainable Growth and Quality Jobs*, Sept. 2009, at 5, available at <<http://www.whitehouse.gov/administration/eop/nec/StrategyforAmericanInnovation>>.

<sup>10</sup> James Manyika & Charles Roxburgh, McKinsey Global Institute, “The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity,” October 2011, at 1, available at <[http://www.mckinsey.com/mgi/publications/great\\_transformer/pdfs/McKinsey\\_the\\_great\\_transformer.pdf](http://www.mckinsey.com/mgi/publications/great_transformer/pdfs/McKinsey_the_great_transformer.pdf)>

<sup>11</sup> “How Dan Kaminsky Saved the Internet”, *The Guardian* (Dec. 3, 2008) available at <<http://www.guardian.co.uk/technology/blog/2008/dec/02/dns-kaminsky>>.

requested, however, is incompatible with end-to-end implementations of DNS Security Extensions (DNSSEC), a critical set of security updates.”<sup>12</sup> DNS Security Extensions, a ten-year project to increase DNS security, has figured prominently in the White House’s strategy for increasing security on the .gov, .edu, and .us top level domains (TLDs).<sup>13</sup> The security experts also noted that any DNS filtering “will pose security challenges, as there will be no mechanism to distinguish court-ordered lookup failure from temporary system failure, or even from failure caused by attackers or hostile networks.”<sup>14</sup> By conflicting with this crucial update to Internet architecture, SOPA thus directly undermines Internet security.

In addition to threatening the Internet’s stability, as well as government and law enforcement intelligence gathering, insofar as DNS filtering is likely to drive users to offshore servers.<sup>15</sup> SOPA’s requirement that domestic DNS servers block certain domain names will encourage users to switch from servers provided by their ISPs over to foreign servers, thus hindering the U.S. Government’s ability to gather intelligence and track potentially dangerous trends in Internet traffic.

These “rogue” DNS servers pose additional threats, as they will be attractive to domestic and foreign users who are unwilling to permit their Internet experience to be dictated by U.S. regulatory preferences. For example, the Pirate Bay began providing its own uncensored DNS server. Users will be told that if they use Pirate Bay’s ‘phonebook,’ they will have a censorship-free experience. Pirate Bay’s ‘phonebook’ may become an attractive nuisance target for cyberattacks designed at exploiting its control over traffic, and it is uncertain whether Pirate Bay or any other ideologically motivated provider of a DNS server will have the requisite security. Such a rogue DNS server might decide to redirect Internet traffic for a political purpose. The result is that its DNS server might one day direct users of ‘bankofamerica.com’ or ‘whitehouse.gov’ to a nefarious, malicious site, rather than their intended destination.

This redirection could also hinder network managers’ ability to both monitor activity over their networks and their ability to get any necessary software patches out to users. In sum, the ease with which users can switch to offshore DNS servers means SOPA’s DNS provision would have

---

<sup>12</sup> Steve Crocker, *et al.*, “Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill,” May 2011, available at <<http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf>>.

<sup>13</sup> White House Strategy for American Innovation: Securing Our Economic Growth and Prosperity (Feb. 2011) Appx. A available at <<http://www.whitehouse.gov/innovation/strategy/appendix-a>>

<sup>14</sup> *Id.*

<sup>15</sup> See Letter from Markham C. Erickson, Executive Director, NetCoalition, to The Honorable Patrick Leahy, Chairman, Senate Committee on the Judiciary 3, *supra* n. 5.

little impact on infringement, while hampering intelligence gathering and law enforcement, and increasing the exposure of the U.S. infrastructure to cyberattack.

## **II. SOPA's Domain-Name Oriented Strategy Will Be Ineffective.**

Like the domain name seizure exercises by ICE, SOPA will have little practical impact on reducing infringement. SOPA's primary strategy is to require that certain Internet intermediaries "de-list" sites from the Domain Name Server ("DNS") system – the virtual Internet "White Pages" that connect web servers' easy-to-remember domain names (like ccianet.org) to their unique IP address number (38.100.17.170). Yet users can simply point their browsers to numeric IP addresses instead of domain names, or easily configure their computers to use one of millions of offshore 'phone books' (DNS servers), thereby circumventing the restriction.

Thus, a SOPA-ordered blockage of 'www.ccianet.org' means that 'www.ccianet.org' will no longer direct users to the IP address 38.100.17.170. The CCIA website will not disappear, however. Instead of typing 'www.ccianet.org' into their browser bar, users can simply enter the 10-digit string that is CCIA's IP address, and access CCIA's website. The blocking order is thus more like an order to tear a page out of a phonebook to prevent people from dialing the "bad" number. The relevant page will be missing from the lone phonebook from which it was removed – the DNS server – but the number still remains in all other phonebooks, and the "bad" phone line – the IP address – hasn't been disconnected. Everyone who has an unaltered phonebook still has the number, and everyone who knows the number may still dial it. Moreover, users can circumvent the blocking order by employing another phonebook (DNS server) through a simple change of their browser settings. Even *supporters* of the domain blocking strategy have conceded that changing DNS servers is "incredibly easy".<sup>16</sup>

When Wikileaks' DNS server was under cyberattack in late 2010, the site's IP address was a top search result on all major search engines, and could also be easily discovered on numerous online forums or in news articles discussing the dispute. Users simply copied "213.251.145.96" into the address bar of their browser and easily accessed Wikileaks. Ultimately, the cyberattack on Wikileaks server which caused the site's domain name to fail had little effect on the availability of the site.

---

<sup>16</sup> Daniel Castro, "No, COICA Will Not Break the Internet," Innovation Policy Blog, The Information Technology and Information Foundation (Jan. 18, 2011), available at <<http://www.innovationpolicy.org/no-coica-will-not-break-the-internet>>.

Our law enforcement experience indicates that targeting domain names specifically has little effect.<sup>17</sup> For example, in June 2010 nine domain names were seized by the United States Immigration and Customs Enforcement Agency (“ICE”) under the banner of a new initiative called “Operation In Our Sites.”<sup>18</sup> Only a few days after the seizure and initiative were announced on a lot at Walt Disney Studios in Burbank, CA, at least two of the seized domains were back online under different domain addresses.<sup>19</sup> After ICE shut down Swedish company TV Shack’s tvshack.net domain, the site’s operators relaunched at tvshack.cc, a domain administered by the Australian territory of the Cocos Islands. Additionally, the seized Movie-Links.tv site was back online at its new www.watch-tv-movies.info address.

In addition to providing little enforcement value, domain-blocking strategies can cause significant collateral damage. Even First Amendment lawyer Floyd Abrams, in a letter ostensibly intended to support the bill, openly concedes that “court-approved remedies under the Stop Online Piracy Act may result in the blockage or disruption of some protected speech.... When injunctive relief includes blocking domain names, the blockage of non-infringing or protected content may result.”<sup>20</sup> Examples illustrating this occurred in November 2010, with seizure of several hip hop blogs, including OnSmash and RapGodFathers.<sup>21</sup> The seizure of these blogs illustrate the tensions between a common marketing technique in the music industry where labels, agents, or artists themselves send popular blogs new songs and videos to post in order to garner attention (also called “leaking”), and the immediate sanctions implemented through ICE’s “Operation In Our Sites” initiative.<sup>22</sup> Similarly, in his recent letter to ICE Director John Morton, Senator Wyden called into question the November seizure of dajaz1.com based on an ICE special agent’s ability to download four songs that were legally provided to dajaz1.com’s operator for purposes of distribution.<sup>23</sup>

Finally, domain names are a blunt instrument for targeting specific content. While in some cases, all of the content of a site will be infringing, in many cases this will not be the case. As

---

<sup>17</sup> One of the only beneficiaries may be domain name registrars, who arguably benefit the most from this enforcement strategy because pirates who must register more domain names will pay more registration fees.

<sup>18</sup> Michael Cieply, “9 Domain Names Seized in Fight Against Internet Theft,” Media Decoder Blog, *N.Y. Times* (June 30, 2010), available at <<http://mediadecoder.blogs.nytimes.com/2010/06/30/in-anti-theft-effort-officials-seize-9-domain-names>>.

<sup>19</sup> Erick Schonfeld, “TV Shack Flouts the Feds by Moving Video Piracy Site to Offshore Domain,” *TechCrunch* (Jul. 6, 2010), available at <<http://techcrunch.com/2010/07/06/tv-shack-piracy>>.

<sup>20</sup> See Letter from Floyd Abrams on behalf of Screen Actors Guild *et al.*, at 11-12, Nov. 7, 2011.

<sup>21</sup> See Ben Sisario, “Piracy Fight Shuts Down Music Blogs,” *N.Y. Times* (Dec. 13, 2010), available at <<http://www.nytimes.com/2010/12/14/business/media/14music.html>>.

<sup>22</sup> *Id.*

<sup>23</sup> Letter from Senator Ron Wyden to The Honorable John Morton, Director, U.S. Immigration and Customs Enforcement 2, *supra* n. 10.

mentioned in the cases of OnSmash and RapGodFathers above, songs and videos are often given to the website by the artist herself, her agent, or even the label. Such “leaking” of new and upcoming material is a common music industry marketing technique to stir up ‘buzz’. SOPA’s endorsement of a domain-name filtering approach threatens to shut down innovative marketing tools such as those described above.

More broadly, SOPA contains few mechanisms to address the overbreadth or undereffectiveness described above. The insistence against exploring more narrowly tailored alternatives, such as a “follow-the-money” approach that has been deployed with success in other areas (most notably, with respect to Wikileaks), is difficult to rationalize given the clear shortcomings and limited effectiveness of an approach that corrupts Internet architecture.

### **III. SOPA’s Overbroad Definitions Sweep in Legitimate Online Sites and Legal Products and Services.**

In an ill-conceived effort to reach not just the “worst of the worst” pirates, but all sites on the Internet engaged in any form of IP misconduct, SOPA stigmatizes any site that “enables or facilitates” infringement, without any analysis as to whether such conduct is knowing or willful. Both Sections 102(a)(2) and 103(a)(1)(A)(i) use either “enable” or “facilitate”, notwithstanding the fact that years of burdensome litigation have shown that iPods, VCRs, personal computers, photocopiers, and countless consumer electronics – in addition to the Internet itself – all *enable* and *facilitate* violations of copyright law. Yet under SOPA’s definitions, legitimate sites selling these electronic products are labeled as pirates, because these provisions of the bill contain no requirement of willfulness or knowing conduct.

Because a site can become a site “dedicated to theft of U.S. property” when it meets any one prong of the definition in Section 103(a)(1), it need not – as some supporters have mistakenly claimed – be “primarily designed” for piracy. A legitimate website may achieve this dubious status merely on the basis of third party marketing, or if it has “taken, deliberate actions to avoid confirming a high probability of the use of the U.S.-directed site to carry out acts that constitute” a violation of copyright law or the DMCA’s anti-circumvention provisions. The peculiar construction of “deliberate[ly]... avoid confirming a high probability” of third party misconduct appears to be improvidently drawn from *Global Tech Appliances, Inc. v. SEB S.A.*, 131 S.Ct. 2060 (2011), where

the “probability” inquiry formed one half of a two-part inquiry, from which the Court concluded a *direct* infringer had actual knowledge of the infringing conduct.<sup>24</sup>

Strangely, unlike Sections 102 and 103, Section 202 of SOPA does require intentional, knowing conduct when it addresses individuals who traffic in inherent dangerous goods or services, or aid drug counterfeiters. Such trafficking must be intentional, and aid to drug counterfeiters must be provided knowingly. Why this less regulatory, narrower, and more reasonable standard is applied in relation to matter that is definitionally more dangerous than infringing copies of football games and Hollywood movies is inexplicable. If there were any justification for the more regulatory approach of burdening those who merely “enable” or “facilitate” conduct, even without knowingly doing so, it would apply in relation to dangerous goods. Yet in this case, the bill requires a knowing, willful conduct.

#### **IV. SOPA Overturns the Digital Millennium Copyright Act.**

SOPA directly conflicts with the Copyright Act’s established and highly successful framework for addressing online infringement, which has been in place since 1998. The Digital Millennium Copyright Act’s (DMCA’s) safe harbors, found in 17 U.S.C. § 512, have stood the test of time, and are in fact codified in more than a half-dozen international trade commitments.

Nearly all U.S. Internet sites, and many foreign sites, invest substantially in DMCA compliance. Although burdensome, this compliance is widely regarded as the cost of entry in being an Internet-based service: a regulatory obligation undertaken by responsible corporate citizens. This construct is so important to the Internet and telecommunications sectors of the United States that it has been incorporated as a bilateral obligation in nearly every Free Trade Agreement (FTA) and Trade Promotion Agreement (TPA) since 2003, including the US-Australia FTA,<sup>25</sup> US-Bahrain FTA,<sup>26</sup> US-Chile FTA,<sup>27</sup> US-Colombia TPA,<sup>28</sup> US-Morocco FTA,<sup>29</sup> US-Peru TPA,<sup>30</sup> the US-Singapore FTA,<sup>31</sup> and CAFTA.<sup>32</sup> More recently, these provisions were mandated by the US-Korea Free Trade Agreement, which, while signed in 2007 and approved by Congress last month, has yet

---

<sup>24</sup> The other half being that “the infringer can almost be said to have actually known the critical facts”. *Id.* at 2071.

<sup>25</sup> US-Australia FTA, art. 17.11.

<sup>26</sup> US-Bahrain FTA, art. 14.10.

<sup>27</sup> US-Chile FTA, art. 17.11.

<sup>28</sup> US-Colombia TPA, art. 16.11.

<sup>29</sup> US-Morocco FTA, art. 15.11.

<sup>30</sup> US-Peru TPA, art. 16.11.

<sup>31</sup> US-Singapore FTA, art. 16.9.

<sup>32</sup> DR-CAFTA, art. 15.11.

to be approved by the Korean legislature. At the same time, U.S. trade negotiators are working to ensure that the same DMCA-like commitments are mandated in the Trans-Pacific Partnership, currently under discussion.

It is in the context of these ongoing international trade negotiations that SOPA proposes a framework that directly flouts these numerous existing international obligations. SOPA does so by directly contradict the language of the DMCA, and also contradicts its core purpose.

*SOPA contradicts the language of existing safe harbors.* One of the established principles of the DMCA is that it is not economically feasible for a site or service to monitor the unfathomable amount of data that crosses a given network, whether that is 1600 tweets *per second* (Twitter), 48 hours of video *per minute* (YouTube), or 10 trillion messages per year (non-spam email, 2010). For this reason, Section 512(m)(1) indicates that a service need not monitor its network or affirmatively seek out infringing activity. While SOPA nominally gives lip service to this principle, it also requires sites and services to “confirm a high probability” that third parties are engaged in infringing conduct – thus imposing an obligation to monitor.

Various technical aspects of SOPA further contradict the DMCA through vague, overreaching, and burdensome language. For example, SOPA requires service providers to take “technically feasible and reasonable” steps to prevent the domain name (or portion thereof) from resolving, but betrays considerable ignorance about Internet operations. Short of a regulatory rulemaking process regarding what is and is not “technically feasible,” this obligation is open-ended, and appears to imply that any feasible technology – such as deep packet inspection – must be implemented to satisfy blocking requests. In addition to constituting a monitoring obligation, this would violate the DMCA’s established prohibition against technology mandates.

Finally, the requirement that all intermediaries must act “expeditiously” – which is defined as compliance within 5 days<sup>33</sup> – is strikingly unrealistic in light of the countless demands placed upon service providers today by law enforcement. The DMCA opted against a definition for “expeditious,” recognizing that the ability of different service providers to achieve regulatory compliance varied, and that “expeditious” compliance for a small garage-based startup would not be the same as that of a large telecom provider.

*SOPA creates broad new liabilities, mooting the very purpose for the protections established by the DMCA.* The DMCA’s primary purpose is to limit the litigation exposure of legitimate sites and services. SOPA creates extensive new litigation exposure. Under SOPA, sites qualifying for the

---

<sup>33</sup> See § 102(c)(2)(A).

DMCA safe harbor may nevertheless be subject to orders from the Attorney General and demands from private parties (including but not limited to IP rights-holders). These sites and services may also be subject to an enforcement order by the Attorney General, and in addition may also be deemed a “site dedicated to the theft of U.S. property” and subjected to lawsuits by foreign and domestic plaintiffs under an *in rem* provision. Insofar as the entire purpose of the DMCA safe harbors was to limit litigation, and SOPA will create more litigation, SOPA moots the DMCA. Thus, while it is true that SOPA does not amend 17 U.S.C. § 512, it renders those crucial safe harbors moot by establishing various new opportunities for plaintiffs to file lawsuits. In doing so, SOPA upends one of the cornerstones upon which our successful Internet economy has been built, and breaks numerous international commitments.

## **V. SOPA Will Undercut U.S. Efforts to Resist Foreign Government’s Efforts to Seize Control of the Internet.**

American foreign policy seeks to promote global Internet freedom, recognizing that a free and open Internet serves the cause of democracy around the world, and simultaneously opening markets for one of America’s fastest-growing export markets. SOPA, however, threatens to be an arrow in the heart of global Internet freedom.

As drafted, SOPA will undermine U.S. efforts to influence global norms affecting the free and open Internet, including in the realm of information regulation and cross-border data flow. In addition to the actual structural risks SOPA poses to DNS servers, SOPA contradicts existing United States diplomatic efforts. SOPA would send a message to foreign nations that overbroad content restriction is permissible when aimed at implementing policy goals. U.S.-sponsored extraterritorial censorship – even for websites perceived to be violating U.S. copyright law – grants a license for other nations to censor at home, and extraterritorially as well. For whatever purpose, noble or otherwise, overbroad censorship of the Internet will encourage reciprocal trade barriers that threaten to fragment the Internet, impair U.S. business interests overseas, and throw a wrench into the machinery of 21<sup>st</sup> century statecraft.

SOPA further encourages problematic behavior already observed abroad by using liability rules to induce online intermediaries to evaluate content and disappear “illegitimate” content. Increasingly, governments aiming to censor do not build a “Great Firewall” like that of China,<sup>34</sup> but

---

<sup>34</sup> Rebecca MacKinnon, “Stop the Great Firewall of America,” N.Y. Times, Nov. 16, 2011, *available at* <http://www.nytimes.com/2011/11/16/opinion/firewall-law-could-infringe-on-free-speech.html>.

‘outsource’ their censorship to the private sector by holding private industry responsible for all information that passing over private sector networks, services, and sites.

One egregious example is a case currently transpiring in Thailand. Chiranuch Premchaiporn, executive director of Thailand’s Prachatai.com website, is being criminally prosecuted for 10 different violations of Section 15 of Thailand’s 2007 Computer Crime Act (CCA) and *lesé majesté* laws for comments posted by third parties which were allegedly disrespectful to Thailand’s monarchy.<sup>35</sup> The allegedly offensive content was removed from the forums as soon as moderators were notified, but prosecutors intend to hold the site operator personally liable from the moment any “disrespectful commentary was ‘imported’ onto systems under her control.”<sup>36</sup> This massive draconian enforcement is not something that the United States should encourage.

Another recent example from abroad is conduct occurring in Sri Lanka. Sri Lanka has blocked five news websites because their reports arguably constituted “character assassination and violating individual privacy” of key political leaders, said Information and Media Ministry Secretary W.B. Ganegala.<sup>37</sup> The U.S. Embassy in Colombo expressed its deep concern in a statement last week, and called for Sri Lankan authorities and telecommunications firms “to stop activities aimed at blocking free access in Sri Lanka to all legitimate media websites.”<sup>38</sup>

The deputization and penalization of intermediaries is a dangerous precedent to set, which will embolden oppressive and authoritarian regimes to pursue policies to the political and economic detriment of the United States. By achieving an extraterritorial application of U.S. law, SOPA will encourage those authoritarian governments seeking greater control over Internet architecture. For example, foreign officials have previously demanding that the ITU, a UN agency, take control of Internet governance functions from the US-based independent non-profit ICANN.<sup>39</sup> India also advanced a recent proposal for the UN to take on Internet governance functions.<sup>40</sup>

---

<sup>35</sup> See O’Brien, Danny, “Holding intermediaries liable for users’ content,” *Committee to Protect Journalists*, Oct. 24, 2011, available at <<http://www.cpj.org/internet/2011/10/cpj-testifies-in-trial-of-chiranuch-premchaiporn.php>> Each violation has a maximum penalty of five years in prison. Crispin, Shawn, “Internet freedom on trial in Thailand,” *Committee to Protect Journalists*, Feb. 4, 2011, available at <<http://www.cpj.org/blog/2011/02/internet-freedom-on-trial-in-thailand.php>>.

<sup>36</sup> *Id.* In 2010, the Thai government ordered that 38,868 websites and Web pages be blocked for publishing anti-royal content.

<sup>37</sup> Mallawarachi, Bharatha, “Sri Lanka blocks 5 news websites over ‘insults’,” *Associated Press*, Nov. 7, 2011, available at <<http://news.yahoo.com/sri-lanka-blocks-5-news-websites-over-insults-094158881.html>>.

<sup>38</sup> *Id.*

<sup>39</sup> Omar El Akkad, “The Internet Needs Peacekeepers. Is Canada Ready?,” *The Globe and Mail* (Nov. 12, 2010), available at <<http://www.theglobeandmail.com/news/national/time-to-lead/internet/the-internet-needs-peacekeepers-is-canada-ready/article1795954/>>.

<sup>40</sup> T. Ramachandran, “India Presses for New Global Internet Governance Mechanism,” *The Hindu*, Nov. 7, 2011, available at <<http://www.thehindu.com/sci-tech/internet/article2604526.ece>>

Sound intellectual property enforcement policy need not compromise our international priorities, however. As Secretary of State Hillary Clinton recently wrote in a letter to Congressman Howard Berman (D-Calif.), it is possible to support enforcement of intellectual property rights online without censoring the Internet. CCIA agrees that there “is no contradiction between intellectual property rights protection and enforcement of expression on the Internet.”<sup>41</sup> For example, the United States promotes online enforcement of rights and protects intermediaries from being secondarily liable for users’ actions under the safe harbors of the Digital Millennium Copyright Act (DMCA). As noted above, these safe harbors are instrumental to U.S. foreign policy, and have been incorporated into our international trade obligations.

The U.S. Government has been promoting these principles in other international fora as well. The Organisation for Economic Co-operation and Development (OECD) is engaged in policy development exercises that involve establishing proper boundaries for intermediary liability. The U.S. Government has invested considerable time and resources in ensuring that OECD policies reflect sound policy and promote U.S. goals, including the well-established intermediary safe harbors in 47 U.S.C. Sec. 230, and 17 U.S.C. Sec. 512. For example, the Final Communique on Principles for Internet Policy Making resulting from the OECD’s June 2011 High Level Meeting on the Internet Economy established that “appropriate limitations of liability for Internet intermediaries have, and continue to play, a fundamental role, in particular with regard to third party content” and reaffirmed the need to “minimis[e] burdens on intermediaries and ensur[e] legal certainty for them.” Overturning the Digital Millennium Copyright Act, or other actions that create uncertainty for intermediaries, undermine these important efforts.

## **VI. SOPA’s Unfunded Obligation Upon the Private Sector to Provide Law Enforcement Support May Violate the Fifth Amendment.**

Unlike most other law enforcement assistance measures, SOPA forces communications intermediaries to provide law enforcement assistance to the government free of charge. Mandating that the private sector provide compulsory service to the Federal Government is uncommon – heretofore largely restricted to federal law enforcement and national security purposes. In any event, such services are almost invariably compensated for at market rates. But whereas law enforcement assistance laws such as the Stored Communications Act and the USAPATRIOT Act amendments all

---

<sup>41</sup> Nagesh, Gautham, November 4, 2011, <http://thehill.com/blogs/hillicon-valley/technology/191895-sec-clinton-no-contradiction-between-web-freedom-and-ip-rights->

reimburse intermediaries at the prevailing rate when they are compelled to provide services,<sup>42</sup> SOPA demands private entities provide free services to the Federal Government, for the protection of *private* government-granted rights, without any reimbursement or compensation to the service provider. As has been noted in relation to the Electronic Communications Privacy Act (ECPA), “[g]overnments have a power of compulsion, and § 2706 [of ECPA] attaches a price tag to the use of that power, just as the Constitution’s takings clause requires compensation for other uses of governmental power to obtain private property.”<sup>43</sup> Particularly with respect to the lawful content that service providers will be ordered to block, governments have no basis for arguing that they are entitled to free services. Mandating the provision of such services without market-based cost recovery may constitute a Taking in violation of the Fifth Amendment.

These burdens are being imposed at a time of increasing demands from federal and state law enforcement for the private sector to provide ever-increasing amounts of information. Existing DMCA regulatory compliance already poses a considerable burden on small and medium sized enterprises, including ISPs and cloud providers. Layering SOPA compliance on top of these compliance burdens, without compensation, would dramatically increase the cost that online services face associated with policing the Internet.

## **VII. Finding Solutions**

The Internet community strongly supports prudently drafted legislation designed to target online infringement. The legitimate services which power the Internet and help drive the U.S. economy have indicated their willingness to shoulder a substantial burden in providing protection and assistance to rightsholder constituencies. This does not include, however, support for an ill-conceived legislative initiative that threatens to undermine the security of the Internet.

Solutions are available. Instead of SOPA’s sweeping regulatory approach, a “follow-the-money” where the third parties who have transactional relationships with bad actors are targeted, would pose no risks to cybersecurity. The Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA),<sup>44</sup> which prevents online gambling web sites from access to credit card payment systems, is one example of this approach. The aforementioned case of Wikileaks is another.

---

<sup>42</sup> See, e.g., 18 U.S.C. § 2706; 18 U.S.C. § 3124(c).

<sup>43</sup> *Ameritech Corp. v. McCann*, 403 F.3d 908 (7th Cir. 2005).

<sup>44</sup> 31 U.S.C. §§ 5361–5367.

According to a recent multi-university study of file sharing networks, less than 100 users were responsible for a large portion of the piracy. Specifically, “a small fraction of publishers were responsible for 67% of the published content and 75% of the downloads,” and were “largely driven by financial incentives.”<sup>45</sup> Addressing the financial motivation to pirate content and counterfeit wares would directly target the root cause of this phenomenon, in a manner that would not undermine Internet security.

## **Conclusion**

CCIA continues to hear concerns from many in our industry who are only just beginning to appreciate the sweeping nature of this mammoth bill, which has been rushed into a hearing with little consultation from the technology and Internet sector. As our industry analyzes the full ramifications of this proposal, we expect to hear many more comments, and it may be necessary to supplement these views in the record.

Because Internet businesses were not consulted on the text of SOPA prior to its introduction, the alternatives noted above have yet to be fully explored. With revision, many of SOPA’s grave shortcomings identified above can be resolved. CCIA looks forward to working with the Committee and its staff to improve this bill and achieve a workable legislative result, which will target foreign rogue websites without extraordinary collateral damage.

---

<sup>45</sup> See Rubén Cuevas *et al.*, “Is Content Publishing in BitTorrent Altruistic or Profit Driven?” ACM CoNEXT (2010), available at <[http://conferences.sigcomm.org/co-next/2010/CoNEXT\\_papers/11-Cuevas.pdf](http://conferences.sigcomm.org/co-next/2010/CoNEXT_papers/11-Cuevas.pdf)>.