Computer & Communications Industry Association
1972-2012: 40 YEARS OF TECH ADVOCACY

SOPA AND ITS IMPLICATIONS FOR TPP

The controversy in the United States over the Stop Online Piracy Act (SOPA) has profound implications for the Trans Pacific Partnership (TPP) agreement. The SOPA debate underscores the importance of striking the proper balance in intellectual property laws to promote creativity and innovation. It demonstrates that over-protection can stifle free expression and the effective operation of the Internet as a medium of communication and commerce not only within a jurisdiction, but also extraterritorially. Additionally, the debate reveals the ability of the Internet community to mobilize quickly to defeat policies that it believes threaten its existence. TPP negotiators should understand the SOPA experience to avoid repeating its mistakes.

The SOPA Controversy

SOPA in the U.S. House of Representatives, and its companion legislation in the U.S. Senate, the PROTECT IP Act or PIPA, attempt to address the perceived problem of non-U.S. websites engaged in infringing activity. Because these so-called "rogue" websites have domain names registered outside of the U.S. (*e.g.*, ".uk" rather than ".com") and are hosted on servers outside of the United States, they are beyond the jurisdiction of U.S. courts and the existing enforcement mechanisms under U.S. law. (SOPA and PIPA are part of a broader enforcement strategy, including the federal government's seizure of hundreds of domain names registered in the United States and criminal prosecutions against the operators of Megaupload.) Although the bills have technical differences, their basic approach is the same. They would require intermediaries subject to U.S. jurisdiction to block access to the foreign websites, or to prevent the flow of revenue to these sites.

More specifically, SOPA and PIPA would authorize *in rem* lawsuits in U.S. courts against a domain name associated with a site dedicated to infringing activity. If the court found that the website met the statutory standard, the court would issue an order which would be served on four categories of intermediaries:

- **Internet service providers** would be required to prevent the domain name from resolving to an Internet protocol address. In other words, when a user typed the domain name of the non-U.S. site into his browser, the service provider would not connect the user to the non-U.S. website.

- **Search engines** (*e.g.*, Google, Bing or other sites that direct users to other online locations) would be required to disable links to the non-U.S. site.

- **Payment systems** (*e.g.*, Visa or MasterCard) would be required not to process payment transactions between customers with U.S. accounts and the account used by the operator of the non-U.S. site.

- **Internet advertising networks** (*e.g.*, Google AdWords or AdSense) would not be able to place advertisements on the non-U.S. site or have sponsored links to the non-U.S. site.

If the intermediaries did not comply with an order, they would be subject to an enforcement proceeding.

SOPA and PIPA provoked the following sharp criticisms from Internet companies and users:

- **Legitimate websites.** Although the bills' sponsors said that they were targeting the "worst of the worst" foreign websites, the bills as introduced applied to both U.S. and non-U.S. websites. Moreover, a small amount of infringing content within a large website conceivably could trigger a remedy that would apply to the entire website. And compliance with the Digital Millennium Copyright Act's notice-and takedown procedures would not provide a safe harbor. Thus, websites that host user generated content, including cloud-computing sites, could be affected.

- **The actions by intermediaries.** All four types of actions required by intermediaries raised concerns.

    - All four required actions, because they were targeted at websites rather than specific content within websites, were blunt instruments that could lead to the termination of service to lawful as well as unlawful content.

    - The domain name and search engine blocking remedies were particularly controversial. Both approaches are used by governments that restrict free expression. Thus, U.S. endorsement of these methods to block access to content that the U.S. government considers illegal (*i.e.*, IP infringing) would legitimate other countries' use of these methods to block access to content they consider illegal (*e.g.*, criticism of the government). Indeed, a letter from Members of the EU Parliament stated that "blocking of websites, by DNS or otherwise, severely undermines America's credibility in the global information society."

    - Domain name blocking also has the potential of introducing cybersecurity vulnerabilities. Court-mandated domain name blocking requires service providers to return authenticated and unencrypted responses to domain name queries in contravention of emerging cybersecurity protocols. Moreover, as users attempted to circumvent the domain name blocking,

they would use foreign domain name service providers that did not comply with U.S. government cybersecurity standards.

- Because both bills allow private rights of action, the volume of cases could be very large, and the intermediaries would need to take action with regard to many sites, at great expense. Intermediaries may decide that simplifying their compliance obligations by eliminating certain services or categories of users will reduce their costs.

- **Technology Mandates.** The bills allow intermediaries to be second-guessed as to whether they took sufficient action to meet their obligations in response to orders. This would invite courts to determine what measures were "technically feasible and commercially reasonable," and mandate additional technological measures by the intermediaries.

- **Due Process.** Under SOPA as introduced, advertising networks and payment systems would be required to terminate service to non-U.S. websites within five days of receiving an allegation of infringement from a rightsholder, without any judicial determination of wrongdoing. SOPA and PIPA include a "vigilante" provision that provides a safe harbor for intermediaries that terminate service to websites in response to rightsholder allegations. However, no mechanism is provided for the website operator or its users to challenge the termination of service.

- **Privacy.** All the problems identified above, taken together, would provide Internet companies with a strong incentive to monitor user activity so as to prevent the possibility of service termination.

- **Extraterritorial Application of U.S. Law**. SOPA and PIPA would impose U.S. IP standards on non-U.S. websites. As the Members of the EU Parliament stated, "[c]onsidering the world wide character of the internet, European companies will be forced to adhere to US standards to avoid DNS blocking." To be sure, the non-U.S. website in theory would have the ability to defend itself in the *in rem* proceeding, but few website operators would be willing to bear the expense of litigation in the United States.

  The domain name blocking and the payment system termination presumably would largely prevent just U.S. users from reaching the non-U.S. site, and thus would have limited impact on the website with respect to the rest of the world. However, the search engine blocking and the advertising network termination could affect the website's accessibility outside of the United States. A U.S. search engine would be required to remove links to the non-U.S. website, which could mean that a non-U.S. user of the search engine would not be directed to that site – even if the user was in the same country as the website! Similarly, a U.S. Internet advertising network would be required to stop placing advertisements on the website – even advertisements that have nothing to do

with the United States. Since the world's largest search engines and Internet advertising networks are based in the United States, the bills could result in a dramatic reduction in non-U.S. traffic and revenue to non-U.S. sites.

Significantly, these sites could well be legal in their host country. Because of the different copyright term limits, some works that are still in copyright in the U.S. are in the public domain outside of the U.S. For example, F. Scott Fitzgerald's *The Great Gatsby* remains in the copyright in the United States although it has entered the public domain in Australia. An Australian site that hosted *The Great Gatsby* and similar works could be subject to SOPA and PIPA even though it was perfectly lawful in Australia. And SOPA and PIPA could prevent non-U.S. traffic and advertising revenue to the site.

Similarly, a non-U.S. website (including the website of a bricks-and-mortar retailer) might have a license to distribute content outside the United States. The website, however, would be subject to SOPA or PIPA because the content was viewable in the United States, where the website operator did not have a license. SOPA and PIPA would interfere with non-U.S. traffic and advertising revenue to the site.

The Current Status of SOPA and PIPA

After introduction, both bills gained many co-sponsors and began to move rapidly through Congress, notwithstanding the concerns raised by many Internet companies and users. A variety of factors then converged in mid-January to halt this progress. Two factors are particularly noteworthy.

First, on January 14, 2012, the White House issued a statement expressing concerns with certain provisions in the legislation. While stating "that online piracy by foreign websites is a serious problem that requires a serious legislative response," the White House stressed that "we will not support legislation that reduces freedom of expression, increases cybersecurity risk, or undermines the dynamic, innovative global Internet."

The statement added:

> **Any effort to combat online piracy must guard against the risk of online censorship of lawful activity and must not inhibit innovation by our dynamic businesses large and small**. Across the globe, the openness of the Internet is increasingly central to innovation in business, government, and society and it must be protected. To minimize this risk, new legislation must be narrowly targeted only at sites beyond the reach of current U.S. law, cover activity clearly prohibited under existing U.S. laws, and be effectively tailored, with strong due process and focused on criminal activity. Any provision covering Internet intermediaries such as online advertising networks, payment processors, or search engines must

> be transparent and designed to prevent overly broad private rights of action that could encourage unjustified litigation that could discourage startup businesses and innovative firms from growing.
>
> The statement then addressed the domain name issue:
>
> **We must avoid creating new cybersecurity risks or disrupting the underlying architecture of the Internet**. Proposed laws must not tamper with the technical architecture of the Internet through manipulation of the Domain Name System (DNS), a foundation of Internet security. Our analysis of the DNS filtering provisions in some proposed legislation suggests that they pose a real risk to cybersecurity and yet leave contraband goods and services accessible online. We must avoid legislation that drives users to dangerous, unreliable DNS servers and puts next-generation security policies, such as the deployment of DNSSEC, at risk.
>
> In closing, the White House stated:
>
> We should all be committed to working with all interested constituencies to develop new legal tools to protect global intellectual property rights without jeopardizing the openness of the Internet…. Moving forward, we will continue to work with Congress on a bipartisan basis on legislation that provides new tools needed in the global fight against piracy and counterfeiting, while vigorously defending an open Internet based on the values of free expression, privacy, security and innovation.

The White House statement validated the concerns of the Internet companies, which had been dismissed by many members of Congress.

The second major factor was an online protest on January 18, 2012, organized by entities with an Internet presence. The English language site of Wikipedia, the online encyclopedia, blocked its content and referred users to information about SOPA and PIPA, and how to contact their Congressional representatives. Google blacked out its logo, and Facebook, Twitter, and Amazon placed prominent notices on their home pages concerning the legislation. All told, over 115,000 websites participated in the protest, with 50,000 blacking out all or part of the site. Users quickly responded. Over 10 million signed petitions protesting the legislation. Three million emails were sent to representatives, and over 100,000 phone-calls were made.

The online protest was widely reported in the traditional media, and all four Republican Presidential candidates condemned the bills during the South Carolina primary debate on Thursday, January 19. The co-supporters of the legislation began to withdraw their support. On Friday, January 20, Senate Majority Leader Harry Reid pulled PIPA off of the Senate calendar, and House Judiciary Committee Chairman Lama Smith, SOPA's lead sponsor, stated that "it is clear that we need to revisit the

approach on how best to address the problem" of foreign infringing websites.

Lessons for TPP Negotiations

The SOPA/PIPA experience in the United States demonstrates three points.

- **IP rules can have a significant impact on legitimate websites.** The Internet democratizes commerce and communications. Platforms such as eBay or YouTube allow individuals and businesses of all sizes to reach large audiences and markets. But IP rules that place too heavy a legal burden on the platforms for user activities, as do SOPA and PIPA, will constrain the growth of this Twenty-First Century medium of trade and discourse.

- **IP rules can affect international trade.** The Internet does not recognize national boundaries. IP rules in one country can affect the operation of websites in another country. SOPA and PIPA would not only impose liability in the United States on non-U.S. websites that may be legal in their host countries; they also would interfere with the operation of these websites in their host countries. Provisions like SOPA and PIPA would allow countries – and indeed, individual companies – to erect trade barriers without following multilaterally agreed procedures with notice and due process.

- **Internet users care deeply about its vitality.** The overwhelming public opposition to SOPA and PIPA generated by just one day of online protests indicates that the members of the public will take strong and immediate political action to protect this medium which has become a central part of their lives at home, school, and work. IP, at least to the extent it intersects with the Internet, is no longer an issue of only narrow technical interest.

These three points have three implications for the TPP negotiations.

- **TPP must not include provisions like SOPA and PIPA.** Paraphrasing the White House statement, the IP chapter in TPP must guard against the risk of online censorship of lawful activity and must not inhibit innovation by dynamic businesses large and small. Across the globe, the openness of the Internet is increasingly central to innovation in business, government, and society and it must be protected. To minimize this risk, TPP must be narrowly targeted only at activity clearly prohibited under existing laws, and be effectively tailored, with strong due process and focused on criminal activity. Any provision covering Internet intermediaries must be transparent and designed to prevent overly broad private rights of action that could encourage unjustified litigation that could discourage startup businesses and innovative firms from growing. TPP should protect global intellectual property rights without jeopardizing the openness of the Internet. TPP should provide tools needed in the global fight against piracy and counterfeiting, while vigorously defending an open Internet based on

the values of free expression, privacy, security and innovation.

- **TPP should prohibit IP provisions with an extraterritorial impact.** TPP should prohibit countries from adopting IP enforcement provisions that would have an extraterritorial impact that diminishes national sovereignty.

- **The transparency surrounding TPP must increase.** If the public feels that the provisions included in TPP jeopardize the openness of the Internet, it will strongly oppose the adoption of TPP. To prevent this from happening, the negotiations concerning the IP chapter must become more transparent. Drafts must be made available online for public comment. The fact that in the past some trade negotiations have had little transparency is irrelevant. The SOPA experience demonstrates that a new era of public engagement in IP policy has begun.

January 30, 2012

For more information, please contact Jonathan Band at jband@policybandwidth.com.

900 Seventeenth Street NW Suite 1100 Washington, DC 20006 Tel: 202.783.0070 Fax: 202.783.0534