2015

Stop Online Piracy Act: The Next Step in Copyright Protection or Censorship of Online Expression

Yue Matthew Ma

STOP ONLINE PIRACY ACT: THE NEXT STEP IN COPYRIGHT PROTECTION OR CENSORSHIP OF ONLINE EXPRESSION?

By Yue Matthew Ma

Table of Contents

If you are an online advocate, you probably still remember the largest online blackout in history on January 18, 2012, on the protest of two bills Stop Online Piracy Act (SOPA)[1] and the PROTECT IP Act (PIPA).[2] Wikipedia's webpage, along with dozens of social networking websites including Craigslist, Twitter, Tumblr, as well as corporate sites such as Linux distribution openSUSE, purposefully went offline.[3] Google almost entirely blacked out its front page logo for US visitors with a message saying "Tell Congress: Please don't censor the web!"[4] As the result of the protest, more than 10 million voters contacted the lawmakers to protest the bills. Two days later, Congress moved both bills to further voting, and has since then, postponed the bills indefinitely.[5]

But why the fuss? In this paper, we will review the contents and status of the SOPA and PIPA bills, the problems they are trying to solve, related laws, and the issues with the bills. While the two bills have been indefinitely "shelved", they are not dead. We will also analyze other laws, both domestic and international, around the issues and assess the potential "return" of the bills.

I. SOPA and related laws

A. Overview of SOPA

The SOPA bill (H.R. 3261)[6] was introduced in October 2011 and was primarily targeted at offshore websites that encourage and abet copyright infringement. It allows copyright holders to seek injunction that would result in the blocking of infringing websites to US viewers. If

[1] *See* Bill H.R. 3261, http://thomas.loc.gov/cgi-bin/bdquery/z?d112:HR03261.
[2] *See* Bill S.968, http://thomas.loc.gov/cgi-bin/cpquery/R?cp112:FLD010:@1(sr039).
[3] *See* http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act.
[4] *See Id*.
[5] *See Id*.
[6] *See* Bill H.R. 3261, *supra* note 1.

enacted, the bill would expand the offense of copyright infringement to include infringement of copyrighted work online via digital transmission or dissemination on a computer network. It would also expand the scope of criminal offenses of trafficking in inherently dangerous goods or services to include counterfeit drugs and goods falsely identified for use in military or national security. The proposed bill requires the owner, operator, or domain name registrant or the domain name registras, to cease and desist further activities constituting specified intellectual property infringement or trafficking offenses. This would presumably have the effect of blocking infringing foreign websites to U.S. users.

The act of "injunction" is a two-step process: (1) the intellectual property (IP) right holder harmed by a site dedicated to infringement and accessible to U.S. viewers first provides a written notification that identifies the infringing party to related payment network providers and Internet advertising service providers that provide services to allegedly infringing site, and request that they forward the notice to AND suspend their services to the identified infringing party. Upon receiving the forwarded notice, the accused party may provide a counter notification explaining that it is not dedicated to engaging in specified violations; (2) if the U.S. payment network provider or Internet advertising service provider fails to suspend its services to the allegedly infringing site or the accused party provides a counter notification, the IP right holder can seek action for limited injunction relief against the owner or operator of the domain name, namely against the domain name registrant and domain name registra, respectively. The bill also requires online service providers, Internet search engine providers, payment network providers, and Internet advertising service providers, upon IP right holder's action or receiving a copy of a court order, to take preventative measures including suspending services from allegedly infringing sites or blocking U.S. users from accessing the foreign site. This presumably would

affect, to name a few, U.S. domain name registras or operators (such as Godaddy, Google, and many others), online service providers (including all web hosting services, social network services), Internet search engine providers (including Google, Microsoft, and many), payment network providers or financial transaction providers (including Paypal, VISA, Mastercard, banks or credit card payment operators), and Internet advertising service providers (including Google advertising services and many other social networking services). These aforementioned providers are all considered intermediaries, through whom the foreign websites are either posting online IP infringing materials or conducting infringing online transactions or trafficking directing to U.S. resided users. These affected providers, however, may be immune from liability if they take actions required by the proposed Act or otherwise voluntarily block access or end financial affiliation with allegedly infringing sites.

The supporters of this bill include the Recording Industry Association of America (RIAA), CBS.com, NBC Universal, Pfizer and several hundred other businesses. However, the bill has also received heavy criticism, largely from the Internet community. Although the bill was later amended to limit the enforcement to only non-US sites that are designed or operated with the intent to promote copyright infringement, a wider agreement still could not be reached, which resulted in the decision by the House Judiciary Committee to postpone the bill's passing.

B. Overview of PIPA

A similar Senate version bill that was introduced in the same year as SOPA and has often been discussed with SOPA together is the PROTECT IP Act (PIPA).[7] It was introduced on May 12, 2011, with the goal of curbing access to rogue websites registered outside the U.S. that are dedicated to the sale of infringing or counterfeit goods. This bill would potentially allow the IP

[7] *See* Bill S.968, *supra* note 2.

right holder or Attorney General to file an action against a registrant of a domain name (including a foreign entity) used by an allegedly infringing web site, the owner or operator of the infringing website, or against the domain name registras. If enacted, it would also allow the court, after receiving the filing, to issue a temporary restraining order or an injunction against the domain name registrant, or owner and operator of the website, requiring him to cease or desist infringing activity if the domain name is used for accessing infringing website from U.S. and directing business to U.S. residents and harming U.S. IP right holders.

This bill would not require IP right holders to provide written notification as in SOPA, and it would also affect financial transaction providers, Internet advertising services, search engines, online directories, and domain name registries and registrars. These parties would be immune from liability, however, if they comply with a court action to take certain preventative measures, or in good faith, voluntarily take certain preventative actions against infringing websites.

The supporters of this bill are mainly content providers and associations such as National Cable & Telecommunications Association, Motion Picture Association of America, RIAA, drug companies and manufacturers. The majority of opponents are Internet community members like Google, Facebook, Mozilla and Wikipedia. Like SOPA, this bill was shelved indefinitely by the Senate shortly after the online protest in January 2012.

C. Overview of DMCA

The Digital Millennium Copyright Act (DMCA)[8] was signed into law in 1998. It implements two World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, and covers other copyright related

[8] *See* http://www.copyright.gov/legislation/dmca.pdf.

issues. Among the relevant sections, Title II of the DMCA: "Online Copyright Infringement Liability Limitation Act", codified into Section 512 of the Copyright Act, now 17 USC §512, creates limitations on secondary liability for copyright infringement by online service providers, and is often referred to as a safe harbor.

To qualify as an online service provider, one's activities must fall into one of the four types: (1) transitory communications - data conduit and transmission of digital information from one point to another at someone else's request; (2) system caching - acts of intermediate and temporary storage through an automatic technical process for the purpose of making the material available to subscribers; (3) storage of information on systems or networks at direction of users; (4) information location tools - hyperlinks, online directories, search engines and the like. A service provider whose activities fall into one of these four categories and meets certain conditions would not be liable for copyright infringement. The conditions are slightly different for each category, but generally include: (a) the provider must not modify the contents of the material, nor determine the recipients of the material; (b) temporary data must impose limited access (e.g. password) and must not be ordinarily accessible to anyone other than anticipated recipients; (c) the provider must not have the requisite level of knowledge on the material being infringed; (d) if the provider has the right and ability to control the infringing activity, he must not receive a financial benefit directly attributable to the activity; and (e) upon receiving a notification of claimed infringement, the provider must expeditiously take down or block access to the material.

The so called "take-down" or "notice & take-down" process works in two steps: (1) a copyright owner submits a notification under penalty of perjury, including a list of required elements, to the service provider so the service provider has sufficient information to locate the

allegedly infringing content and the subscriber who posted it; (2) the service provider would then promptly remove the material and notify the subscriber that it has been removed. To prevent possibility of erroneous or fraudulent notification, the subscriber can file a counter notification to the service provider stating under penalty of perjury that the material was removed by mistake. Then, the service provider has 10 - 14 business days to put the material back unless the copyright owner files a court action against the subscriber. The statute gives special treatment to nonprofit educational institutions whose faculty or students might post infringing materials on institution's website. Under such special treatment, the educational institution would be eligible for the safe harbor, and could further receive up to two notifications in the next three years before they are considered to have had requisite knowledge of faculty member or student's infringing activities. Further, providing online access to certain recommended course materials would not be considered infringing activity.

This statute affords service providers with a safe harbor, under which they are exempted from liability to any person if, upon receiving a proper notification, they promptly remove or block access to the material identified in the notification. At the same time, the statute also imposes an obligation on service providers to comply with the notice & take-down provision. Otherwise, they could face legal consequences.

II. Why the fuss with SOPA and PIPA?

A. What problem is SOPA/PIPA trying to solve?

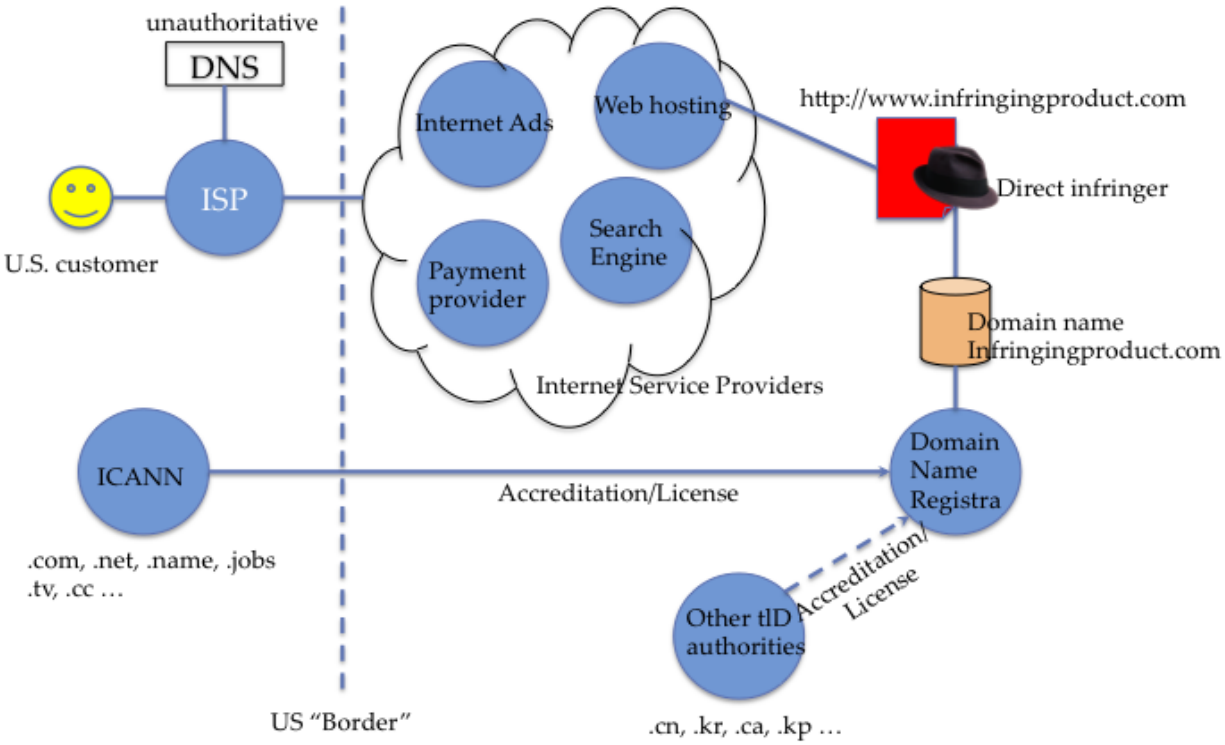

Figure 1. Topology of Internet.

Both SOPA and PIPA attempt to curb access to non-US websites that are designed and dedicated to harming the U.S. economy by facilitating transmittance or selling of infringing materials or products online. The difficulties with non-US websites are the lack of reach of U.S. legal enforcement in stopping infringing activities, and SOPA/PIPA proposes solutions that would block these non-US websites to U.S. users. To comprehend SOPA/PIPA's approach, we must first understand how the website and Internet work and what various players come into the picture.

With reference to Fig. 1, suppose you were running an infringing website called www.infringingproduct.com. You would need to do two things: one is to obtain your domain name infringingproduct.com, and the other is to set up a website to post your contents related to infringing product or services. To obtain your domain name, you would register with a domain name registra. The top-level domain.com in this example is managed by a nonprofit organization in the U.S. called Internet Corporation for Assigned Names and Numbers (ICANN), headquartered in L.A., California, but you would not need to register with ICANN directly. ICANN accredits and distributes licenses to several hundreds domain name registras worldwide (e.g. GoDaddy, Google, or foreign organizations) that handle domain name registration and maintenance. When you register your new domain name with a local accredited domain name registra, you become a registrant or owner of the domain name. After registration, you would create the contents of your website and have it hosted by a website hosting service. Your contents would be physically located on the server of your website hosting service, and everyone in the world would be able to access them. Alternatively, you could forgo hosting and host your website on your own. You could rent an Internet line with a static IP address and set up a server machine in your basement. The process is relatively simple and inexpensive. You can host your own website anywhere in the world and have it accessible to the entire Internet including users in the U.S. Suppose you do sell infringing products to U.S. customers, you are doing commerce with U.S. and hurting U.S. economy, but the U.S. court system can not easily get to you because all of your domain name registra, your website and even yourself can be physically located outside the U.S.

SOPA/PIPA also considers ways your website could reach a U.S. customer. With reference to Fig. 1, suppose a U.S. customer signs up an Internet service with a local company

(e.g. Verizon, Comcast) that becomes his Internet Service Provider (ISP). If the customer knows your website, www.infringingproduct.com, he can directly enter the website name in his browser. His request first reaches his ISP's domain name server (often called the unauthoritative domain name server), which translates the requested domain name to a real IP address by contacting other domain name servers on the Internet, and eventually reaches the root domain name server, which maintains the actual record of domain to IP address mapping for your domain. Upon getting the real IP address, the U.S. customer obtains access to your infringing website from his browser. So this simple browsing action involves at least two parties: the local ISP of the U.S. customer who is likely maintaining the unauthoritative domain name server and the root domain name server where the actual record of domain name is maintained. The former is on the U.S. customer side, and the latter is likely on the infringing party's side, whichever country it may be.

There is another complication to this structure. Most of the time, the U.S. customer does not know the name of the infringing website or is not even aware that he is accessing an infringing website that may be outside the country. Instead, the customer simply searches for the product he is interested on the Internet, and an advertisement or the search engine ends up leading him to visit the infringing site. Further, if he purchases the product from the infringing website online, another third party, either payment network or financial transaction provider, such as PayPal, VISA or Mastercard, will have to complete the transaction process. Thus, many parties could all participate in promoting and assisting with the infringing activity.

SOPA and PIPA attempt to hold all these parties liable unless they take reasonable measures to block the U.S. customer from linking or communicating to the foreign infringing website and cut of the source of funding to these sites. In short, SOPA/PIPA could certainly go

after the owner or operator of the domain name and infringing website, and if not possible, hold all third parties on the U.S. side liable.

B. Comparison of SOPA, PIPA and DMCA safe harbor

SOPA/PIPA and DMCA both enforce secondary liability on indirect infringing parties who facilitate the direct infringing party with or without knowledge. But, there are also differences among the approaches and intended objectives of these statutes, as illustrated in Table 1.

Table 1. Comparison of SOPA, PIPA and DMCA Safe Harbor.

	SOPA	PIPA	DMCA Safe Harbor
Objective	Targets only non-US sites that are designed or operated with the intent to promote copyright infringement and counterfeit sales (amended)	Targets sites that have no significant use other than engaging or facilitating infringement and selling counterfeit goods	Targets subscribers posting infringing materials on a website
Approach	Copyright holder sends notice, then can sue direct infringing party, or third party if the third party does not take preventive measures	Attorney General or copyright holder can bring action against direct infringing parties, and if they are unreachable, can take down domain name that is used by infringing activity	Copyright holder can send notice to service provider to request a take-down, then service provider shall take down. Subscriber can counter notice and engage in legal action
Targets (Direct Infringing)	Owner or operator of domain name or website	Owner or operator of domain name or website; domain name itself (both domestic and non-domestic domain name)	Subscriber who post infringing materials on the Internet
Other third parties accountable (Indirect Infringing)	Internet search engines, financial transaction providers, internet advertising services, domain name registras	ISP, financial transaction provider, internet advertising services, providers of information location tools (search engine, online directory, other online links)	Service provider (no knowledge of content, no control of recipient) – including search engine, file sharing, web hosting etc.
Action required of 3rd party for exemption	To take preventive measures upon receiving court order	To take preventive measures upon receiving court order or AG order	To take down accused content immediately; no financial benefits from the infringing activity

DMCA seems to focus narrowly on accused parties posting infringing materials on websites and holds all relevant third parties liable unless they are shielded by the safe harbor. DMCA is also broad in a sense that it does not specify whether the contents are domestic or overseas. As a matter of fact, 37% of notices sent to Google target sites outside of the U.S. [9] Along that line, SOPA/PIPA similarly target non-U.S. websites that are designed and dedicated to conducting infringing activities while engaging U.S. Internet users, yet relevant non-U.S. parties could not be reached by conventional U.S. law enforcement. This problem is certainly not being addressed by DMCA's safe harbor provision. Therefore, SOPA/PIPA proposes to track down to the source of the domain name used by the infringing website, and if the domain name is outside U.S., to trace to the end U.S. customer who requests access to the website. Besides requiring providers in the social network to take down infringing contents or remove all links to an infringing website that could reach each U.S. customer, SOPA/PIPA also requires local ISPs to filter out domain names used by infringing websites, thus blocking their access by U.S. customers. This approach is certainly more stringent than DMCA.

C. What are the issues with SOPA/PIPA?

The response to the proposed SOPA and PIPA is enormous. While most supports are from IP right holders e.g. entertainment industry including media content providers, cable companies, and pharmaceuticals who vested in their own interest of protecting from infringing activities, the majority of the Internet community is quite negative. Some of the major concerns include:

(1) The proposed bill could lead to censorship on the Internet and other constitutional issues

[9] *See* The DMCA Process (Infographic), http://blog.nexcess.net/2012/02/22/dmca-process-infographic-flowchart/.

One reason for Congress' push for SOPA/PIPA was their success in Internet blocking in the United States v. American Library Association.[10] In *ALA* the Supreme Court held that Congress' enactment of the Children's Internet Protection Act (CIPA), where the CIPA requires that "public library may not receive federal funding to provide Internet access unless it installs software to block images that constitute obscenity or child pornography and to prevent minors from obtaining access to material that is harmful to them", was constitutional, While CIPA protects children in public libraries and public schools from exposure to obscene or otherwise harmful material, incidentally blocking more material than was appropriate were considered harmless mistakes. In comparison, SOPA/PIPA's target audience is radically different and much broader. Under SOPA/PIPA, the traditional powerful copyright holders would be able to label sites as persistent infringement inducers and shut them out from the most lucrative market in the world. By extending duties to third party payment processors and advertises, SOPA/PIPA puts a lot of power in the hands of the government and IP right holders that could potentially lead to significant abuse and harmful mistakes. It could also lead to the creation of blacklists and censorship of the Internet for other purposes. Further, it has been well-established that domain name is a property, thus the removal of web sites from the Internet would be considered property seizure with the accused website or domain name owners being unrepresented. This raises the issue of the government removing protected speech from the Internet.

(2) The proposed bill is taking away the DMCA safe harbor provision

DMCA has already afforded protection for the copyright holders under provide notice & take-down provision, requiring service providers to take proper measures upon receiving written notification from a copyright holder, who has properly identified the infringing website. Under

[10] *See* 539 U.S. 194 (2003).

DMCA, copyright owners who object to the use of their specific content may trigger an individual response by issuing a take-down notice, whereas a significant minority of copyright owners are now perfectly happy to share their work online without receiving remuneration or requiring advance approval. DMCA's safe harbor provision further exempts online service providers from liability should they promptly follow the notice & take-down procedure. Opponents of the SOPA/PIPA argue that DMCA has already achieved the effect intended by the new bill, and therefore, the new bill is taking away safe harbor protection for service providers.

(3) The new bill could hurt innovation

Under the proposed bill, the providers who designed tools and provided means for generic Internet use for all activities could be forced to monitor the type of activities being conducted on the Internet. While the types of activities conducted are often at the whim of the user, these providers could face secondary liability for infringing contents posted by their users, thus the bill poses undue burdens to various Internet players. In particular, this can hurt Internet start-ups and social media sites or even impede venture capitals from investing in Internet content intermediaries businesses.[11]

III. Traditional legal enforcement on secondary liability

Secondary liability of copyright infringement has long been addressed by the traditional legal system, with Internet file sharing being one of the most active and representative areas. We will analyze several notable cases through the evolution of file sharing technologies and understand how laws have been applied. We will also analyze a more recent Court of Appeals

[11] *See* Five ways SOPA/PIPA would impact Web start-ups, by Olga Khazan, http://www.washingtonpost.com/blogs/on-small-business/post/5-ways-sopapipa-would-impact-web-start-ups/2012/01/18/gIQAPWFF8P_blog.html.

decision on Flava Works, which sheds some lights on whether the current law protects copyright holders against "third tier infringement" activities.

A. Napster the pioneer of file sharing

Napster was perhaps the first popular peer-to-peer (P2P) file sharing system, by which people were freely sharing files, mostly MP3 music files online. It was during the beginning of the millennium, when most people thought that one could never sue end users for downloading files or third parties for providing the tools. However, the powerful record industry fought relentlessly, and it is now well established that illegal distribution and download of copyrighted music by individuals can result in criminal penalties. The music industry has also successfully sued Napster for contributory and vicarious infringement and the court ordered injunction against Napster.[12]

In *A&M Records v. Napster Inc.*,[13] the court held that Napster was liable for both contributory and vicarious infringement for they had facilitated user's infringing activity, and they had benefited financially from pushing advertising streams to the users. In comparison to MP3.com, which committed the fatal error of actually hosting songs on its own servers, Napster instead only hosted the directories and links on its server, not the actual files. However, the court found that Napster had the knowledge and intent to induce infringement. Furthermore, although one who would otherwise be liable for contributory and vicarious infringement could use the DMCA safe harbor to avoid liability, the court held that Napster would not be entitled to the DMCA safe harbor even though they had not received an official take-down notice from the copyright holders. The court made it clear that the DMCA safe harbor could not protect the defendant when he is clearly abetting and encouraging infringement en masse.

[12] *See* A&M Records v. Napster, Inc., 239 F.3d 1004 (9th Cir. Cal. 2001).
[13] *See Id*.

B. Grokster wave

Napster was shut down, company's assets were liquidated, yet the Napster brand survived. Later, other companies followed the P2P file sharing example. Unlike Napster, who maintains control over the transaction of file transfer through maintaining directories and links on a central server, Grokster's architecture is different, because they invented computer "root supernodes", which reside in users' computers. Each supernode functions as a hub to enable file transfers to/from user's computers without going through Grokster's servers. Although Grokster won partial judgment in their favor in both district court and Court of Appeal, the Supreme Court unanimously held that Grokster could indeed be sued for infringement for their activities and using Grokster service for copyrighted materials is illegal.[14] Under the same doctrine of *A&M Records v. Napster, Inc.*, the court held that one who distributes a product, capable of lawful and unlawful use, with clearly shown object of promoting copyright infringement is held liable for copyright infringement by third parties using the product. Although the Grokster case did not address the DMCA safe harbor, there was much contention over whether Grokster was entitled to the SONY safe harbor[15] for non-infringing activities (SONY was not liable for infringement because of substantial non-infringing activities associated with the use of its recording devices). Clearly, no safe harbor would be available for exemption of secondary liability if a party were obviously promoting infringing activity.

C. Bittorent wave

In the turning of this decade, another wave rose with the spread of the Bittorent file sharing protocol, by which files are not transferred from a single source or as a single file. Instead, a file is broken into segments called pieces that can be distributed to an unlimited

[14] *See* MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (U.S. 2005).
[15] *See* Sony Corp. v. Universal City Studios, 464 U.S. 417.

number of users whose computers could serve as a server. This totally decentralized approach enables a user to download pieces of a file from different sources at different times and to eventually receive a file in complete form. File transfer is usually facilitated by Bittorent tracker websites that provide searching of files and coordinate the file distribution. Since the metafile provided by a tracker does not include any part of the copyrighted content itself, but rather a link to a possible source of one of the pieces, the issue is whether or not a tracker violates copyrights. However, in a case against Megaupload,[16] a HK based Bittorent tracker, the court dismissed Megaupload's motion to dismiss the direct and contributory infringement claim. The court held that Megaupload served as more than a passive conduit or file storage, and it created a distinct website presumably in an effort to encourage or pay its users to upload a large amount of popular media while being aware of the ongoing infringement taking place on its websites. Doubts have been raised among different courts as to whether a take-down notice automatically implies knowledge (to exclude the defendant from the safe harbor),[17] however, the fact that Megaupload had actual knowledge about the infringement activity but did not do anything excluded them from being entitled to the DMCA safe harbor. After the court's denial of Megaupload's motion to discuss, the parties settled. Later, the United States Department of Justice seized and shut down the file-hosting site Megaupload.com and commenced criminal cases against its owners and others. The next day Hong Kong Customs froze more than US$39M of the company's assets. On the same day, the New Zealand police arrested Megaupload's founder and three other executives upon the U.S. FBI's request.

[16] *See* Perfect 10, Inc. v. Megaupload Ltd., 2011 U.S. Dist. LEXIS 81931, 2011 WL 3203117 (S.D. Cal. July 26, 2011).
[17] See Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 50067, 2011 WL 1791557, at *3 (N.D. Ill. May 10, 2011).

D. Flava Works: Grunt was not infringing

After *Megaupload* had settled, the court vacated its decision at the request of the parties, but another district judge criticized the decision as well. Certainly, a case could become murkier when a service provider participates less and less in the infringing activity. The *Flava Works*[18] case pushed the question even further as to how far the current law can go in protecting a copyright holder's rights and to what extent of protection DMCA gives the copyright holder by holding a third party liable. Flava Works is a producer of gay pornography videos and owns several businesses including video streaming off its website. The defendant Gunter owns a social networking and video sharing website myVidster.com, which allows users to post, bookmark and share links to their favorite videos. By clicking on the shared link, a user would be able to watch the video online by streaming from the source through an embedded frame only on myVidster.com's server without saving a copy anywhere. In *Flava Works*, Judge Posner of the Court of Appeals of the Seventh Circuit reversed the district court's decision and held that Gunter was not liable for contributory infringement of Flava Works' copyrighted works because providing underlying bookmarkers were not copyright infringement. Posner made an analogy of the instant case to the conduct of someone sneaking into a movie theater and watching a copyrighted movie without buying a ticket, which conduct is illegal in some other aspects but not copyright infringement. The court further held that there was no evidence that myVidster incentivized its users to infringe. The court also held that even if myVidster did not comply with DMCA notice & take-down provision, such non-compliance was not evidence of wrongdoing or relevant – "a noninfringer doesn't need safe harbor."

[18] *See* Flava Works, Inc. v. Gunter, 689 F.3d 754.

In comparing *Grunt* to *Napster* and *Grokster*, do these cases bear some resemblance, since the defendants all enabled and coordinated users to share copyrighted materials without maintaining any copies on the server? The only difference between the defendants is that Napster and Grokster allow users to download a file copy, while Grunt allows users to only share links of videos with others. Yet, the former two were deemed liable for contributory infringement and the later was not. But is this difference really significant enough to justify opposite outcomes? What if *Napster*, *Grokster* or *Megaupload* had all changed their architecture to restrict their users to only watching copyrighted materials online without downloading a copy, would they be legitimate? Or did Judge Posner's leniency in the *Grunt* case have anything to do with the nature of the Flava Works' contents as obscene? See Devils Films,[19] where the court was unwilling to exercise its equitable powers to benefit a plaintiff who sold obscene, hardcore pornography films, and denied the plaintiff's application for an order of seizure and preliminary injunction under the strong public policy against the distribution of obscene materials.

After more than a decade of legal battles on file sharing, the law still has uncertainties, yet it has been well established that (1) secondary liability for copyright infringement against a third party does exist and (2) DMCA safe harbor would not be viable if a defendant had clear knowledge of and was clearly encouraging infringing activities.

IV. Is SOPA/PIPA the best approach?

A. SOPA/PIPA has substantial overlap with conventional laws

The objective of SOPA/PIPA is to prevent non-U.S. websites designed or dedicated to conducting infringing activities from reaching the U.S. customers. Let's look at the several laws we just visited and see how they apply.

[19] *See* Devils Films v. Nectar Video, 29 FS2d 174 (SDNY 1998).

DMCA safe harbor can only reach service providers. If the infringing activity is conducted on a U.S. website, a U.S. copyright holder can confront the website operator or provider using the DMCA notice & take-down provision. If the website operator does not take down the infringing content, the copyright holder can bring action to the operator through the conventional U.S. court system. If the website operator is offshore, the U.S. copyright holder can still go after other service providers within the meaning of DMCA safe harbor including search engines and online directories that provide U.S. customers with links to the infringing website (under information location tools prong), Internet advertising providers (could be under system caching prong), and financial transaction providers or file sharing facilitators (could be under transitory communication prong). The copyright holder may send notice to request that these parties take down the infringing contents.

If the facilitator or promoter of the infringing website is not a service provider within the meaning of DMCA or is a service provider but does not comply with the notice & take-down procedure, the copyright holder can still sue him in a U.S. court. A U.S. court would have personal jurisdiction over a foreign entity if the foreign entity has minimum contact in the U.S.[20] For example, Megaupload regularly conducts business in U.S. and takes payment from U.S. customers thus has established minimum contacts. It is therefore subject to personal jurisdiction in a U.S. court. Further, under *Grokster* and *Megaupload*, DMCA safe harbor would not exempt someone from liability if he clearly had knowledge of infringing activities, and within its control, promotes, encourages, or facilitates the infringing activities.[21]

But within the U.S. court system, if the defendant does not physically reside within the U.S. or has no agents residing in the U.S., can the plaintiff still serve the defendant? There would

[20] *See* International Shoe Co. v. Washington, 326 U.S. 310 (1945).
[21] *See* MGM Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (U.S. 2005).

be reasonable means of serving for most of cases. Federal Rule of Civil Procedure 4(f)(1) allows the use of internationally agreed means of service authorized by the Hague Convention on the Service Abroad of Judicial and Extrajudicial documents. The Hague Convention on the Service is a much more simplified means of serving documents than diplomat letters. The Hague Convention Service has about 70 or so signatory countries, including China, Egypt, Russia, Pakistan, many other European, South and Latin American countries, and Australia. If a defendant does not reside in Hague signatory countries, F.R.C.P. 4(f)(2) still allows a method that is reasonably calculated to give notice by the foreign country's law for service.

Proponents of SOPA/PIPA realized a loophole that has not been addressed by the convention systems. Even if we cut all the cords that tie to the foreign website conducting infringing activities, the foreign domain name and websites are still out of reach, and the U.S. customers can still have access to those websites directly. SOPA/PIPA proposes to do two things: (1) to seize the domain name; and (2) to force the local ISP of the U.S. customer (unauthoritative domain name server) to stop translating IP addresses for a domain name on the blacklist so that U.S. customers can not reach the infringing website. This is essentially a domain name filtering or censorship of the Internet. The enforcement against unauthoritative domain name servers does not seem to be available in any other existing laws. However, the seizure of foreign domains is already available in the existing statute: the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP),[22] and 18 U.S.C. ss. 981 and 2323, which later enabled Department of Homeland Security's Operation in Our Sites.

PRO-IP was enacted into law in 2008 out of the concerns of P2P file sharing. It increases both civil and criminal penalties for trademark, patent and copyright infringement. The PRO-IP also permits the Department of Justice to conduct civil suits on behalf of copyright holders, and

[22] *See* http://en.wikipedia.org/wiki/PRO-IP_Act.

in criminal enforcement, gives the government more authority in seizure and forfeiture in the trafficking of counterfeit goods.[23] In the Bittorent wave, the Department of Justice used PRO-IP to seize and shut down the domain Megaupload.com. In seizure of domain names, PRO-IP appears to be an effective means, except that it could not reach any property outside the U.S. This may not be a huge issue because the most popular top-level domain .com is overseen by a U.S. organization ICANN, who also owns many other popular top-level domains such as .net, .name, .job, .tv, .cc etc. For those country specific top-level domains such as .cn (for China), .kr (for Korea), .ru (for Russia), .kp (North Korea), PRO-IP would not be effective.

The Operation in Our Sites[24] is a venture conducted by Immigration and Customs Enforcement's (ICE) under the Department of Homeland Security to seize domain names for infringing copyright. ICE may obtain a seizure warrant issued by a United States District Court under the authority of 18 U.S.C. ss 981 and 2323, which permits the civil forfeiture of property involved in certain criminal transactions including copyright infringement. The ICE has been operating for some time, and included in their 2010 release[25] of seized domain names were related to a diverse array of counterfeit goods such as handbags, shoes, sports equipment, athletic apparels, illegal copies of copyrighted DVD boxes and well-known BitTorrent tracker site Torrent-Finder.com. All seized domain names were either .com or .net, both within the control of ICANN. In a subsequent Operation known as Operation In Our Sites 2.0, ICE seized another 85 domain names including Puerto 80's domain names, rojadirecta.org and rojadirecta.com, which were allegedly used to commit criminal copyright infringements, namely, the streaming of

[23] *See Id.*
[24] *See* http://www.aaronkellylaw.com/internet-law/operation-in-our-sites-legalities/.
[25] *See* http://www.ice.gov/doclib/news/releases/2010/domain_names.pdf.

copyrighted broadcasts of sporting events.[26] Later, Puerto 80 challenged the seizure in the District Court for the Southern District of New York and petitioned for return of its domain names,[27] but their petition was denied by the District Court.

Based on the aforementioned analysis, most of the problems the SOPA/PIPA is trying to solve can be addressed by various statutes under the existing U.S. legal system, except when the infringing website is using a foreign country specific top-level domain, and the U.S. customers can still directly access the infringing website through unauthoritative domain name servers.

B. Is SOPA/PIPA going to be effective in achieving its intended goal?

We have shown that existing laws in the U.S. system can mostly address the problem intended to solve by the SOPA/PIPA. Thus, the questions are (1) whether SOPA/PIPA can effectively solve the problem that cannot be solved by the conventional laws; and (2) whether the overall SOPA/PIPA approach is feasible.

(1) SOPA/PIPA cannot effectively solve the problem that can not be solved by the conventional laws

The enforcement of SOPA/PIPA on ISPs would require Internet service providers to use a DNS filtering to blackout pirate websites from the U.S. customers. Proponents of the bill argued that filtering is already common and that the effect of this requirement on business would be minimal. This may be true. However, if a customer knows the physical numeric IP address of the infringing website, he could also visit it directly without having to go through a domain name server, completely bypassing the DNS filtering. Even if the numeric IP address becomes public

[26] *See* EMERGING ISSUES IN INTELLECTUAL PROPERTY, MEDIA, AND HIGH-PROFILE DEFENSE LAW: ARTICLE: Catch Me if You Can: An Analysis of New Enforcement Measures and Proposed Legislation to Combat the Sale of Counterfeit Products on the Internet, 32 Pace L. Rev. 567

[27] *See* Puerto 80 Projects, S.L.U. v. United States, No. 11-3390-cv, 2011 WL 6148823 (2d Cir. Dec 6, 2011).

and ends up in the blacklist, new websites can be launched fairly quickly via redirection technology. Internet redirection technologies would allow a website to reappear under a different name within a matter of hours after it is being blocked, and would still be able to reach the U.S. customers' homes. Thus, DNS filtering could not block a website entirely.

(2) The overall SOPA/PIPA approach is only doubtfully justified

As stated previously, the SOPA/PIPA overlaps with existing U.S. laws substantially. The innovation of SOPA/PIPA is the DNS domain filtering at the very end of the Internet traffic flow, i.e. the local ISPs of the U.S. customers, yet it still could not block an infringing website entirely. For this narrow and imperfect solution that SOPA/PIPA could offer, the price to pay by the U.S. tax payers and consumers is certainly high and unjustified. First, how each ISP should maintain the blacklist would require continuous efforts to dynamically update the blacklist in order to keep up with the activities. As all filtering technologies have always been, domain name filtering tends to go either "underboard" or overboard, resulting in some undesirable consequences. Second, there is no accurate reliable source to confirm how many ISPs there are in the United States, but it was estimated to be 3,000 - 4,000 around year 2007[28] and could reach over 10,000 today. This means that implementing SOPA/PIPA would require enormous amounts of resources. Internet service providers are already among the most hated companies in the U.S.[29] as the cost of their data service is several-fold higher than in some other countries. To comply with SOPA/PIPA, the ISPs are likely to pass on the cost to their customers or degrade the services, potentially impeding technology development.

Then the issue becomes how much damage has been caused by infringing websites operating outside the U.S., using non-ICANN controlled domain names whose infringing

[28] *See* http://askville.amazon.com/ISPs-United-States/AnswerViewer.do?requestId=524267.
[29] *See* http://www.huffingtonpost.com/2013/05/22/internet-service-providers-hated_n_3320473.html.

activities can not be effectively sanctioned by existing U.S. legal system. In the Senate Report of PIPA,[30] the Senate reported some statistics from research reports on American job and money loss caused by counterfeit products. For example, "each year, copyright piracy from motion pictures, sound recordings, business and entertainment software and video games costs the U.S. economy $58 billion in total output, cost[s] American workers 375,375 jobs and $16.3 billion in earnings, and costs Federal, State, and local governments $2.6 billion in tax revenue." Other numbers on damages were also cited in the report.

However, the numbers provided by the legislators do not give enough details as to justify SOPA/PIPA. The damage amount did not break down as to the amount of damage that has been caused by counterfeiting activities in the U.S. which can already be addressed by existing U.S. laws, and the amount of damage caused by operations outside the U.S. using non-domestic domain names. If legislators are targeting infringing websites operating from China, Russia, Cayman Island, or any other territories outside the U.S., they should provide the numbers on damages sustained in those regions, respectively. Since the SOPA/PIPA overlaps substantially with other laws, there should be a study on the effectiveness of those laws in the past to evaluate and justify the enactment of a new law. However, the legislators have not provided statistics on the effectiveness or the recovery of damages from implementing other related laws such as DMCA, PRO-IP etc. Furthermore, the loss of revenue due to piracy and counterfeit always seem to be overestimated by the industries with vested interests of IP rights. If all Americans who buy counterfeit products are stopped from doing so all of a sudden, would every single person in that group buy or be able to afford buying the corresponding brand name products? If all the channels of buying counterfeit Rolex watches are cut off, will people who intended to buy a counterfeit

[30] *See* http://thomas.loc.gov/cgi-bin/cpquery/?&dbname=cp112&sid=cp1125HUNm&refer=&r_n=sr039.112&item=&&&sel=TOC_1858&.

switch to buy the genuine Rolex at the retail price? Without these numbers, we would not be able to estimate the tangible merit from this new bill as measured against its cost.

For the narrow protection that would be added to the existing legal system, for the benefit that seems to be far outweighed by the cost of implementation, and for the lack of reasonably foreseen recovery, SOPA/PIPA would not effectively achieve its intended goal.

V. Anti-counterfeiting online is an international approach

So far we have been analyzing anti-counterfeiting entirely within the U.S. system, which does not seem to provide a perfect solution. Yet, today's Internet has become more and more ubiquitous and borderless. Internet can reach almost anywhere in the world. For example, a top-level domain name .com can be registered by anyone in the world; a website regardless which domain name it is using can be hosted on a physical server anywhere. There are hundreds of domain root servers and thousands to tens of thousands unauthoritative domain name servers, and proxy servers distributed worldwide, coordinating all the web traffics. It is not apparent to an Internet user where the website he is visiting is physically located, who is managing it, and what Internet components operated by whom has helped him to reach the site he is visiting. In this ubiquitous and borderless Internet world, it becomes clear that the lawmakers attempting to conquer counterfeiting or piracy online must not be limited to conventional approaches. The law enforcement can no longer stay behind a closed door, as the effort must be international in order to be effective. International efforts are already reflected in some of the existing international frameworks, including DMCA enforcement in other countries, TRIPS international agreement, and Internet censorship laws in some countries.

A. International efforts on DMCA enforcement

After the DMCA was enacted into law by the U.S. in 1998, other countries followed. Now, many Berne Convention countries, including U.S., China, South Korea, South Africa, Taiwan, and many European countries, have enacted notice & take-down provision in each respective country's law. Several other countries such as India, Canada, Russia, do not currently have notice & take-down procedures.[31]

The protection afforded by the DMCA is not limited to the geographical location of the copyright holder. For example, YouTube, Facebook, and search engines such as Google, all open their take-down procedures to users regardless of their geographical location. In the same token, if someone's copyrighted work is being infringed outside the U.S., in a country where DMCA is being enacted, she would be entitled to take advantage of the notice & take-down. For example, if you discovered counterfeits of your product being sold on the Internet in China, and also actively marketed to U.S. customers, then the Internet service providers (ISP) hosting the infringing website are subject to both China and U.S. law, regardless of where the website is physically located. The law in either country would give you the ability to submit a take-down notice to an ISP to request the ISP to take down the infringing contents from the website, otherwise they would be subject to potential liability under the DMCA.

The international recognition of DMCA gives copyright holders broader protection not only in the U.S. but also in other participating countries as well. The notice & take-down procedures in these countries are similar. They all require the notice to identify the copyrighted work claimed to have been infringed, the specific URL of the infringing contents so the ISP can

[31] *See* http://theipexporter.com/2013/03/25/enforcing-online-copyright-protections-abroad-understanding-foreign-takedown-notice-requirements/.

properly locate it, specific request to take down and rights holder's contact information. However, there are some differences among these countries. For example, China requires rights holders to submit preliminary evidence of infringement, while the U.S. requires rights holders to state their good faith belief of infringement under oath.

B. TRIPS agreement for international copyright protection

The agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) is an international agreement negotiated in 1994, and administrated by the World Trade Organization (WTO). It provides enforcement, remedies and dispute resolution procedures for the protection of a variety of forms of IP rights covering content producers, performers, producers of sound recordings and broadcasting organizations, patents, IC design, trademarks, trade dress, trade secret and new plant. This agreement now has 158 parties (all WTO members) and has already established a good framework that has been accepted by all signatory countries. There is certainly no need to reinvent the wheel. While TRIPS ties IP protection to trade policy, it could be an effective vehicle to push each country for a vastly more effective enforcement mechanism with which to hold each other accountable. There are also criticisms and controversies surrounding TRIPS, particularly on some terms being broad and difficult to enforce under each country's respective law (e.g. whether software and business methods are patentable and entitled to protection). One way to get around this problem would be to narrow down the provisions of TRIPS and define a narrower standard that would provide more predictability for copyright holders as well as web sites hosting content.[32]

[32] *See* NOTE & COMMENT: IP WARS: SOPA, PIPA, AND THE FIGHT OVER ONLINE PIRACY, 26 Temp. Int'l & Comp. L.J. 303.

C. Internet censorship by country

China government's censorship on the Internet has been known for decades with the government's target mainly on human rights activists and pornographic contents. This "Great Firewall" regime was the cause of Google's withdrawal from the mainland China market three years ago, because Google and the Chinese government could not reach agreement on Google providing uncensored web contents.[33] This also sent a message to the public on Chinese government's intent to post restrictions on the Internet use. And, they did censor Internet use - Facebook and YouTube are blocked to Chinese Internet users.

Russia's government has also been censoring the Internet for various purposes. There were even protests against the Russian government's arbitrary use of anti-extremism law to target journalists.[34] In late 2012, it enacted a new law to blacklisting websites that the government determined to have illegal content including drugs, suicide and child porn.[35] Later, the government used the new law to request that Facebook, Twitter and YouTube remove certain pages related to suicide, to which Facebook and Twitter complied, and YouTube, owned by Google, resisted.[36]

With the boom of the Internet and social networking, it has become a clear international trend for governments, including that of the U.S., to tighten Internet censorship worldwide. Recently, Reports Without Borders has listed five enemies of the Internet countries including: Bahrain, China, Iran, Syria, and Vietnam.[37] Freedom House has surveyed 60 countries in 2013 and reported in its 4th edition Freedom on the Net that the Internet censorship in 60% of the

[33] *See* http://www.newyorker.com/online/blogs/evanosnos/2012/01/the-chinese-view-of-sopa.html.
[34] *See* http://en.rsf.org/report-russia,131.html.
[35] *See* http://www.forbes.com/sites/reuvencohen/2012/11/01/russia-passes-far-reaching-internet-censorship-law-targeting-bloggers-journalists/.
[36] *See* http://www.nytimes.com/2013/04/01/technology/russia-begins-selectively-blocking-internet-content.html?_r=2&.
[37] *See* http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf.

countries has worsened over the last year, with about a quarter of the countries having no Internet freedom, and half of the countries having only partial freedom.[38] The infrastructure of Internet censorship already exists in many countries, as each government imposes Internet censorship in its respective country for various purposes. To protect U.S. IP rights online, the U.S. government could explore engaging in conversations with governments of the countries that are source of the infringement and counterfeiting problems, to utilize those countries' Internet censorship infrastructure to enforce protection of U.S. rights.

VI. How is SOPA going forward?

Given all the issues previously discussed, the potential return of the SOPA/PIPA bill is quite low, or at least the new bill would have to be of a substantially different format. In our opinion, legislators have to analyze the problem SOPA/PIPA is trying to solve in a finer granularity and limit the scope of the provision to specifically target the narrow problem, and at the same time incorporate international laws and coordinate efforts in attacking counterfeit problem globally. Particularly, the following issues must be examined:

A. Assess the country-specific loss of profit and existing laws in each respective country

As the scope of the current SOPA/PIPA bill is broad and overlaps substantially with the existing laws such as DMCA, TRIPS, PRO-IP, the new bill needs to focus on the specific problems that existing laws could not reach. These existing laws are already in place and have already worked. The proponents of the new bill need to provide concrete numbers as to how much loss of profit suffered in each of the foreign country/region of concern. For example, what's the loss of profits or intensity level of infringing activities out of websites from China,

[38] *See* http://en.wikipedia.org/wiki/Internet_censorship_by_country.

Russia, Cayman Island or anywhere else? What are the domain names used by most infringing activities e.g. .com, .net, or other domain names out of the control of ICANN?

The Senate report of PIPA gives some data on overall lost in the U.S. economy from copyright infringement, but this general number is not sufficient. All existing laws, both domestic and international, have been drawn to repair this damage, and they have been effective. The question now is how much damage has been sustained from the problems that the existing laws could not solve. Without such a clear picture of where the biggest loophole is we will never be able to effectively fill that hole or justify ourselves in giving copyright holders broader protection than what existing laws currently afford.

Once we divide the damage by region, the existing laws in each respective region and their effectiveness when applied to current issues must be assessed. For example, China is a signatory country of both WTO and DMCA and is obliged to comply with the TRIPS and DMCA notice & take-down provision. Russia does not have notice & take-down procedure in compliance with DMCA, nor is it a participant of TRIPS. In 2001, a Russian programmer Dmitry Sklyarov developed a software tool in Russia that allows users to strip the usage restriction of the ebook.[39] While it is legal in Russia, he was arrested in the U.S. while attending a conference and jailed for 9 months for allegedly violating the DMCA.[40] It may be true that the goal of SOPA/PIPA is more difficult to achieve in Russia than in China, however, we are only speculating as to which country may be the most problematic. Again, pinpointing the damage by country would help give a bigger picture of the problem, direct our efforts to develop an effective tool, and allow us to reliably predict its effectiveness.

[39] *See* http://www.adobe.com/aboutadobe/pressroom/pressreleases/200108/elcomsoftqa.html.
[40] Later, the U.S. government dropped all charges against him on the condition that he testify at the trial of his employer, which were ultimately acquitted of any DMCA violations.

B. Explore the existing laws that may encompass enforcement on the specific problems being intended to solve

Legislators should thoroughly explore the existing laws that may have already encompassed enforcement on the specific problems they are trying to solve and evaluate their effectiveness. For example, DMCA notice & take-down provides a simple procedure that allows copyright holders to request take-down of copyright infringing materials without expensive legal routes. It has been adopted by many countries, and thus can also be utilized to enforce take-down of content from a website residing in those countries. Further, the U.S. legal system allows a U.S. court to have personal jurisdiction over a foreign entity as long as the foreign entity has minimal contact in the U.S. within the meaning of FRCP 4. This requirement would be met in most of the infringing activities we are concerned with. In addition, under the PRO-IP and 18 U.S.C. ss 981 and 2323, the government would have authority to seize nondomestic domain names for copyright infringement or counterfeiting. This seizure could be particularly effective since U.S. controls the majority of top-level domains through ICANN. This approach has also been shown to be effective in some notable actions against Bittorrent trackers residing outside the U.S. and those conducted by ICE's Operations In Our Sites. Legislators should also assess the effectiveness of International Trade Commission (ITC) in preventing copyright infringing product and services from entering the U.S. border.

Anti-counterfeit measures against infringing activities originating from outside the U.S. must be an international effort in order to achieve these goals. The proposed SOPA/PIPA approach is tantamount to blocking a fire from entering one's own yard instead of neighbors working together to put out the fire. Without such international efforts, SOPA/PIPA will only endlessly try to keep up with new problems and constantly fill up holes. Legislators should thoroughly assess the related law enforcement in each country we are concerned with. The first

step would be to look at each country's obligation under TRIPS and if necessary, leverage the U.S. position in trade to strengthen the enforcement of copyright protection and request such country to take action. Second, even if TRIPS is not available in a certain country, the U.S. government may request to utilize that country's Internet censorship infrastructure, if any, to achieve the goal of protecting U.S. copyright holders' rights. This action should not be interpreted as the U.S. wanting to encourage these Internet censorships.

C. Assess the technical feasibility

It is known that technologies of Internet blocking are available. But, people who are blocked from accessing certain websites based on their geographical location can still find ways to visit the website via proxy servers. Moreover, certain websites that are filtered by domain name servers can still reappear with redirection technology. These technology flaws are certainly not well thought out in the current SOPA/PIPA proposal. Legislators should thoroughly examine the technical feasibility of methods tailored to solve their specific problems. Internet and social networking may be the fastest growing industry with new technologies being constantly developed. Legislators need to proactively look at potential problems that may arise from using future foreseeable technologies so as to develop a long-term steady solution that is ready for future circumvention instead of simply reacting to old problems.

From technical point of view, the new measures should also take into consideration the ever-growing security concerns on today's Internet and social networking, and make sure security is not compromised. With regard to domain name filtering, legislators should also assess the number of existing and future ISPs, estimate the resources needed to have them properly trained and equipped with proper tools as well as maintain a centralized blacklist to attack counterfeiting activities.

D. Legislators need to be extremely cautious before putting more power in the hands of copyright holders

The DMCA notice & take-down has already given copyright holders a great power in taking down allegedly infringing contents without court procedures. However, it has also created potentials of abuse, when there are valid fair use defenses. Under DMCA, even if a defendant has a fair-use defense, his contents will be taken down before he has an opportunity to rebut. In other words, the reverse damage to the defendant is already done – a result that would not have happened under the conventional legal system where experienced judges first assess the likelihood of infringement before an injunction can be effectuated. Congress succeeded in *ALA*[41] in forcing public libraries to install Internet filtering as a condition for getting government funding, however, the scope of *ALA* holding is limited to the power of Congress and the liability of public libraries. The scope of the SOPA/PIPA is to extend the power to any copyright holders, and would impose liability not only on the direct infringers but also on numerous third parties. If SOPA/PIPA wants to give more power to copyright holders, they need to address all possible copyright infringement defenses (e.g. fair use, estoppel, latches, independent creation), other general affirmative defense, and provide proper education to IP rights holders before enacting the law.

Most importantly, the new legislation has to balance the specific problem it's solving with other legal issues being raised with respect to freedom to speech and free Internet use. The narrow issue arising from the SOPA/PIPA bill is the constitutionality of domain name filtering without due process, where copyright holders can trigger a unilateral action on blocking a domain name. Is such act of domain name filtering justified against the rights of the domain holder, their possible defenses, the undue burden on all the local ISPs and service providers, and

[41] *See supra* note 10.

effects on Internet innovations, because start-ups are now afraid of being held liable for something they do not know?

VII. Conclusion

It is clear that SOPA/PIPA has not been well thought out, and is not the best solution for the problem it had intended to solve. It has substantial overlaps with the existing laws both domestic and international. For the narrow protection it seeks from infringing activities by websites using a nondomestic domain name, the proposed solution of domain name filtering is far from being completely effective, yet it would require enormous amount of resources to implement. The committee notes stated that the SOPA/PIPA bill tries to give "Department of Justice and rights holders an expedited process for cracking down on rogue Internet sites by targeting the domain names associated with those sites through injunctive relief", however, this provision is not clearly justified as to how it is aligned with the specific loss of profit, regions where occurred, and estimate of the effectiveness of the approach.

The likelihood of the return of SOPA/PIPA may be quite low, however, if it comes back, it will have changed substantially. Particularly, legislators need a more thorough analysis as to what narrow problem they are solving, the corresponding damage sustained in each problematic region, existing laws, both domestic and international, and their effectiveness, and feasibility of seeking international efforts. Engaging directly with other countries where the infringing activities originated will not only protect IP rights holders' interests in the U.S., but also give them broader protection outside the U.S.