

Enforcement of Intellectual Property Rights Abroad in a Post SOPA World: OPEN and its Alternatives

Written for:
Sen. Maria Cantwell, Sen. Mark Warner

December 2012

Ryan Lau, MIT
David Campos, MIT
William Stueck, MIT
Andrew Dorne, MIT

With Special Thanks to:
Emery Simon, Business Software Alliance
6.805 Staff, MIT

Table of Contents

Executive Summary.....	3
Introduction	6
Online Piracy Background: Defining Intellectual Property and Online Piracy	6
Peer-to-Peer and Other Piracy Problems of Today	6
The Stop Online Piracy Act	8
Background	8
Targeting the Weak Spots.....	8
Opposition to the Legislation	9
Proposed Solution	11
A Base: The Online Protection and Enforcement of Digital Trade Act	11
Support for OPEN	11
Opposition and Concerns.....	12
Our Proposal: Modifications to OPEN	14
Specific Modifications to the current version of OPEN (H.R. 3782)	14
Solution Analysis.....	18
Transferring USITC Authority to the DOJ.....	18
Removal of §1201 Enforcement – Copyright Circumvention.....	20
Focus on Targeting Payment Processors.....	21
Evaluation of Proposed Solution	24
A Course of Inaction	24
Reviving past legislation	24
Modified OPEN.....	26
Conclusion	27
Appendix I: Example Technological Solution	28
Recommended Technological Approach	28
Current Approach	28
Global Copyright Database	28
Role of the Department of Justice	33
Next Steps	33
Appendix II: A Brief History of Peer-to-Peer Piracy.....	34
Sources	36

Executive Summary

This document describes the current state of the online piracy legislation, specifically pertaining to for-profit websites outside of US jurisdiction, and makes recommendations on the modification of existing legislation that is currently being introduced. The Online Protection & Enforcement of Digital Trade Act (OPEN) is currently the best platform for passing this type of legislation, but it could benefit from the several modifications.

We recommend that several modifications be made to OPEN, and that the modified bill be presented before the legislative branch and key members of the online community. The modifications we propose are as follows:

- **Returning the authority to the Department of Justice from the US International Trade Commission (USITC).** The Department of Justice (DOJ) is a larger organization, and has the expertise and ability to issue cease and desist orders that are more forceful in an expedited manner. ,The USITC has a spotty track record at best when it comes to enforcing patent disputes, and has not demonstrated that it is ready to take on the responsibility of this role.
- **More flexible cease and desist orders given to payment processors.** Payment processors currently cooperate with the government across a range of functional capabilities from drug enforcement to fraud protection. Payment processors are able to determine bad actors across several aliases based on patterns of behavior, but are often loathe to do so because current cease and desist orders lack flexibility. Giving payment processors the ability to target multiple users based on a single cease and desist order and indemnifying them from liability will encourage them to step up their efforts. This is to be balanced by a streamlined

appeals process that allows legitimate users to have their privileges quickly reinstated in case of a “false positive.”

- **Removal of 1201 Copyright Circumvention clause.** Section 1201 has proven very difficult to enforce domestically, and has not had a significant impact on piracy: the distribution step is the true bottleneck for piracy. Furthermore, it is unclear that international enforcement of this clause is worthwhile, and we are concerned by its potential for abuse. Including this in the law only distracts from OPEN’s mission.
- **Focus on targeting payment processors primarily through a clearly defined court procedure.** In order for payment processors to cooperate fully, it is vital that the procedure by which they receive cease and desist notices be as clear and predictable as possible. A robust appeals process and a clearly defined set of protections and indemnifications should be put in place before payment processors will be comfortable with the system. Furthermore, consistency of the law and its application is especially important given that technically the payment processors’ involvement is largely voluntary and in good faith.

In addition, technological solutions are another way to address the problem, and an example automatic monitoring system is proposed. The purpose of this technological proposal is not to give an exhaustive or comprehensive “to-do” list, but rather act as an inspirational thought experiment.

It is clear that copyright enforcement is a key issue that needs to be addressed by the US government, and important steps that have been taken domestically under the Digital

Millennium Copyright Act (DMCA). This piece of legislation ensure that copyright holders have the ability to quickly tag and identify offending material while ensuring that there is a degree of due process that allows the accused parties to defend their interests as well. However, due to the interconnected nature of the Internet, it is crucial that a similar amount of thought be put into legislation addressing foreign “bad actors”. The goals of copyright enforcement legislation are important, and that they can be safely accomplished without majorly inconveniencing innocent users. The improvements that OPEN makes over previous legislation by reducing the scope of the legislation and the severity of the enforcement methods are commendable but do not go far enough. Several changes must be made to the legislation to improve its efficacy, and should be weighed and considered as appropriate in discussions of the legislation.

Introduction

To keep the United States competitive, it is important that content creators be compensated for their work. The internet has created a new distribution network that has made sharing copyrighted materials extremely easy, and while domestic efforts to combat copyright infringement have done reasonably well, international enforcement remains a challenge. Specifically, the global nature of the Internet and the lack of U.S. jurisdiction outside of its borders makes it difficult to enforce international copyright. Legislation such as the Stop Online Piracy Act (SOPA) attempted to address this issue, but failed to become law. The goal of this proposal is to address the issues associated with enforcing US copyright abroad specifically targeting for-profit websites. A new proposal, the Online Protection and Enforcement of Digital Trade Act (OPEN) shows promise as it has support from major detractors of SOPA, as well as from SOPA's original supporters. However, several modifications need to be made to OPEN before it becomes law to make sure that it is maximally effective. This paper recommends changing the language of SOPA to address several key issues.

Online Piracy Background: Defining Intellectual Property and Online Piracy

In general, most copyrighted material in the US gives the owner exclusive rights, to the object in question, be it a movie, song, book or other form of copyrighted material. Online Piracy, without context, is a broad term that connotes any form of copyright infringement conducted on the Internet. Infringement consists of acts done without permission of the rights holder to the work that are not excused by exceptions and limitations under the law, principally fair use.² This would include violations ranging from an individual emailing a friend an MP3 copy of a song, to large-scale Peer-to-Peer (P2P) distribution systems that distribute copyright-protected material. For the purpose of this paper, 'Online Piracy' is defined as the online reproduction and/or distribution of a copyrighted file without the permission of the rights holder and not otherwise permitted by fair use or other provisions of the Copyright Act.

Peer-to-Peer and Other Piracy Problems of Today⁷

Presently, much of the online copyright infringement occurs over Peer-to-Peer (P2P) networks.⁸ These networks are decentralized, and allow users to share files with each other. The most prominent network today is the BitTorrent network. The BitTorrent network allows file transfers through the use of many small data requests over different Transmission Control Protocol (TCP) connections in a random, rather than sequential approach⁹. Essentially, BitTorrent allows a user to receive many small pieces from a pool of users that already have the file (known as seeders) selected at random making tracking these interactions very difficult. Due to its decentralized nature, it is the most

² United States Copyright Office, Definitions. <http://www.copyright.gov/help/faq/faq-definitions.html>

⁷ For a more detailed history of Piracy, see Appendix II

⁸ Brown University Computing and Information Services. *Copyright Infringement*. <http://www.brown.edu/cis/policy/copyright.php>

⁹ Bittorrent.org. *The BitTorrent Protocol Specification*. http://www.bittorrent.org/beps/bep_0003.html

difficult type of piracy to stop. Notable hosts such as ThePirateBay have proved difficult to shut down for a variety of reasons, including foreign server hosting and hosting in the cloud. Cloud hosting is particularly worrisome, as a BitTorrent service provider can keep a website online and engage in illegal activities without the hosting service ever being aware of it. If the hosting service does somehow become aware of infringing behavior, it is extremely easy for the BitTorrent service provider to relocate to a new host.

Additionally, the advent of widespread broadband Internet has allowed a number of streaming services to emerge. With a high-speed Internet connection both legal and illegal access to live TV, movies, and music has become prevalent. On one hand, a number of legal options exist including Hulu and YouTube, which are supported through licensing and advertisement networks. However, illegal websites have become just as commonplace, including FirstRowSports¹¹, Channel 131¹², and One-TV¹³. While legal action has been taken against some websites, such as the US-hosted versions of FirstRowSports, US law enforcement struggles against many of the websites as they are often hosted abroad.

Because these websites are hosted on foreign servers, the US does not have jurisdiction or the ability to provide takedown notices to Internet Service Providers (ISPs). Under the Digital Millennium Copyright Agreement (DMCA), rights holders can, with the assistance of the Federal Government, send takedown notices to ISPs for domestic websites. ISPs will then generally comply with the takedown notice to avoid losing “safe harbor” protections that keep it from being sued. The party that posted the offending material then has a chance to contest the action and show that it had the right to post the material in question. As the U.S. government lacks the authority to enforce these actions abroad, and foreign governments are seldom willing to comply with what is essentially a U.S. mechanism¹⁴, it is clear that a mechanism for enforcing copyright abroad was needed.

¹¹ <http://www.thefirstrow.eu/>

¹² <http://www.ch131.so/>

¹³ <http://one-tvshows.eu/>

¹⁴ Some countries, such as New Zealand in the MegaUpload case have cooperated extensively with the U.S. government. Many other foreign governments have not cooperated.

The Stop Online Piracy Act

Background

House Judiciary Chairman Lamar Smith introduced the Stop Online Piracy Act (SOPA) to the US House of Representatives in mid-2011. A corresponding US Senate bill, PROTECT IP Act (PIPA) was introduced at nearly the same time. SOPA, which this paper will focus on as an example of a failed attempt at a solution, was designed to address the issue of copyright infringement on for-profit, foreign-hosted websites.¹⁶ It received strong support from a number of groups, including major production companies, media companies, and Hollywood, all of whom have a significant interest in maintaining exclusive rights to the material they produce.

The rationale behind SOPA came from the lack of enforceability discussed previously, and difficulties encountered by the U.S. Immigrations and Customs Enforcement (ICE) copyright enforcement action “Operation In Our Sites,” which focused on the seizure of approximately 800 websites that sold counterfeit goods and copyrighted materials.¹⁷ However, all these websites were domestic or under the jurisdiction of cooperating foreign governments. SOPA was developed to create other methods of hurting the bottom line of infringers abroad.

Targeting the Weak Spots

The legislation targeted three main bottlenecks of foreign websites’ business model: the payment processors, advertiser networks, and Internet Service Providers (ISPs). These bottlenecks were chosen because they are largely U.S.-based and thus are under jurisdiction of the Federal Government. By arresting the flow of cash from users and advertisers to the websites, SOPA aimed to make these websites financially untenable. Through the payment processors, SOPA sought to make moving money between infringing clients and hosts impossible. Whether it was credit card companies or alternative processors such as Paypal, the goal was to prevent target websites from receiving money for their infringement actions. The payment processors supported this action, as they did not want to be associated with fraudulent parties. Advertiser networks also represented a key bottleneck in the profitability of infringing websites. Infringing websites often drove their revenue by displaying advertisements alongside their core content, similar to many other online businesses. However, forced compliance had a mixed response from advertising networks, as their revenue is directly related to the placement of advertisements, irrespective of content.

Infringing websites can also be targeted by attacking their distribution networks, and causing ISPs to regulate the content they carried. Online piracy negatively affects ISPs by

¹⁶ HR 3261. *The Stop Online Piracy Act*.
<http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3261>:

¹⁷ Singer, Bill. “Bah Humbug! ‘Operation In Our Sites’ Nabs 150 Websites On Cyber-Monday.” *Forbes*, November 28, 2011, sec. Investing. <http://www.forbes.com/sites/billsinger/2011/11/28/bah-humbug-operation-in-our-sites-nabs-150-websites-on-cyber-monday/>.

the significant bandwidth usage it incurs. Video streaming and downloading consumes a significant amount of bandwidth due to the sheer amount of data that must be transmitted. As such, the prevalence of online piracy leads to either a lower level of service for other customers or increased costs for the ISPs who are required to improve infrastructure in response. SOPA would have allowed ISPs to block access to certain websites through Domain Name System (DNS). DNS, sometimes likened to a phone directory, redirects browser requests from www.example.com to the IP address of the www.example.com hosting server. Meaning, when a user types in a web address, it redirects their request to the appropriate IP address. Under SOPA, ISPs would be required to block websites that had been determined to be infringing, and would not direct a user's request to the relevant IP address. ISPs would be required to keep track of a list of these infringing websites, and actively work to block US traffic from accessing infringing websites. However, targeting ISPs is generally considered a poor solution, as pirate websites can easily move to another domain name and another server at minimal cost. Furthermore, the process places an unfair burden on the ISPs. Given that the ISPs needed to look for the pirate website again and go through the entire shutdown process, this approach is very time consuming and minimally effective.

SOPA relied on a two-step relief process for rights holders whose copyright had been infringed upon.¹⁸ The first step required the rights holder to directly notify the payment processors and advertising networks of the infringing content. Subsequently, the payment processors and advertising networks would be required to stop payments and notify the infringing website, which in turn had the option to provide the copyright holder an explanation for why the website was not actually infringing. If the rights holder found the explanation unsatisfactory, or none is given, the rights holder could move forward and seek a court-ordered injunction against the website's operator.

Opposition to the Legislation

SOPA was very strongly opposed by a wide variety of groups.¹⁹ Spearheading the anti-SOPA campaign was a strong contingent of notable and popular websites, including Google, Wikipedia, and Reddit. These websites cited the potentially overbroad reaches of the legislation, and suggested that the passing of SOPA could result in a forced shutdown of their operations. Under language of the proposed bill, any website thought to be "facilitating" copyright infringement could be shut down. Payment processors and advertising networks would have five days to stop service to the infringing website, at which point the infringing website would need to seek a court order to have its services restored.²⁰ Furthermore, a single incidence of copyright infringement would cause the entire website to fall under the jurisdiction of SOPA and be eligible for a shutdown. Because websites like Reddit and Wikipedia include many links to outside websites and

¹⁸ House Judiciary Committee. *Stop Online Piracy Summary*. October 26, 2011.

<http://judiciary.house.gov/issues/Rouge%20Websites/Stop%20Online%20Piracy%20Summary.pdf>

¹⁹ Fahrenthold, David A. *SOPA Protests Shut Down Websites*. Washington Post.

http://www.washingtonpost.com/politics/sopa-protests-to-shut-down-websites/2012/01/17/g1QA4WYl6P_story.html

²⁰ Pepitone, Julianne. *SOPA Explained*.

http://money.cnn.com/2012/01/17/technology/sopa_explained/index.htm

it is possible that at least one of these links was to an infringing website, it made them vulnerable. Moreover, many of the websites were largely concerned with the potential burden that SOPA could place on them to fight piracy, as it would remove the protections provided to them as a content hosts by the DMCA.²¹ Under SOPA, websites would have to strictly monitor content being published. As some of the most-visited websites in the world, their campaigns (which for many included a one-day blackout) led to strong public opposition and increased awareness of SOPA.

Independent organizations also cited major concerns for the legislation. Free speech advocates, such as the ACLU, believed that the government could use the act to censor controversial material and violate First Amendment rights of citizens.²² They claimed action could be taken against material in a way that could potentially circumvent the content-neutral requirement of the First Amendment.²³

Another provision, DNS blocking, encountered stiff opposition from many technical activists and the White House, and even lost the support of some of SOPA's supporters. As a result, it was quickly removed from the bill provisions.²⁴

Under mounting public opposition fueled by activist efforts, the bill was stopped in House Judiciary Committee discussions. This event was precipitated through the unified protest against SOPA on January 18th by a number of major websites, at which point several Congressmen expressed opposition to the bill.²⁵ With the halting of SOPA and PIPA, legislative action against online piracy has been substantially delayed.

²¹ Center for Democracy and Technology. *Intermediary Liability: Protecting Internet Platforms For Expression and Innovation*. April 2010. [https://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_\(2010\).pdf](https://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf)

²² American Civil Liberties Union, *Urge Congress to Stop SOPA*. December 14, 2011. <http://www.aclu.org/blog/free-speech/urge-congress-stop-sopa>

²³ University of Missouri – Kansas City Law School. *Time, Place Manner Regulations*. <http://law2.umkc.edu/faculty/projects/fttrials/conlaw/timeplacemanner.htm>

²⁴ Fitzpatrick, Alex. *Hollywood: SOPA's DNS Blocking 'Off The Table'*. January 17, 2012. <http://mashable.com/2012/01/17/mpaa-sopa-pipa/>

²⁵ Melvin, Jasmin. *SOPA Stopped After Unprecedented Protests*. Reuters. January 20, 2012. <http://news.nationalpost.com/2012/01/20/sopa-stopped-after-unprecedented-online-protests/>

Proposed Solution

A Base: The Online Protection and Enforcement of Digital Trade Act

In response to mounting criticism against SOPA, two versions of The Online Protection and Enforcement of Digital Trade Act (OPEN) were introduced to each of the houses of Congress. In the House, Rep. Darrel Issa (R-CA) introduced H.R. 3782²⁶, while in the Senate, Sen. Ron Wyden (D-OR) introduced S. 2029.²⁷ OPEN attempted to address the issue of online piracy without the controversy SOPA caused.

OPEN included the following provisions:

- Targeted Internet Sites Dedicated to Infringing Activity (ISDIA)
- ISDIAs must have foreign domains, conduct business for US residents, and engage primarily in infringing activity
- Requires claims be directed to US International Trade Commission (USITC)
- USITC must no longer pursue claims against domestic domains and, only if necessary, refer to Attorney General (AG) office for injunctive relief or prosecution under appropriate law for domestic domains
- If USITC finds violations for ISDIAs, cease-and-desist notices are served to the website, payment processors, and advertisement networks
- Requires payment processors to take reasonable action against completion of transactions to website
- Requires advertisement networks to take reasonable technical measures to cease serving advertisements to which the networks and ISDIA earn revenue
- Unlike under SOPA, advertisers and payment processors are not compelled to act by a certain date, and the DOJ can at most seek injunctive relief against any person subject to a cease and desist order or an advertising or payment network who willfully fails to comply with an order, if the USITC has reached a ruling and rights holders cannot use the USITC ruling in a civil suit
- Provides immunity to advertisement networks and payment processors for reasonable actions to fulfill requirement
- Only after non-compliance from notice can USITC refer case to AG for injunctive relief
- The President is authorized to reject any violation notices found by the USITC

Support for OPEN

A number of SOPA opponents have expressed support for OPEN, including a number of Congressmen and Senators, as well as several prominent Internet and technology companies, including Google, Facebook, Yahoo, EBay, and Mozilla.²⁸ This is key, given that organizations such as Google were some of the most vocal and influential dissenters

²⁶ US. H.R. 3782. *Online Protection and Enforcement of Digital Trade Act*. <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3782>:

²⁷ US S. 2029. *Online Protection and Enforcement of Digital Trade Act*. <http://thomas.loc.gov/cgi-bin/query/z?c112:S.2029>:

²⁸ AOL Inc. et al. Letter to Chairman Darrell Issa and Senator Ron Wyden. Originally published on www.keepthewebopen.com.

to the earlier attempts at legislation. The change has developed for a variety of reasons, including adding the USITC as an intermediary between victims and courts, the elimination of targeting ISPs, and strict limitations against prosecuting domestic domains.²⁹ Furthermore, rights holders can no longer directly target ISPs or advertising and payment networks in civil suits using the USITC rulings.

Adding the USITC as an intermediary increased support from several groups by addressing concerns of judicial overreach. Rather than having a judge, who may not be as particularly well-versed or concerned with trade ramifications, the legislation adds in a third party. The USITC is an organization that primarily handles trade disputes including Intellectual Property claims. The USITC adds an extra layer of knowledge and protection against government overregulation and addresses the concerns of many of the initial opponents. Many of the bill's new supporters view the involvement of the USITC as positive because it is a step towards preventing unnecessary and potentially harmful actions towards websites such as Wikipedia, which expressed concern over shutdown for having a single page with infringing content.³⁰

Moreover, adding strict limitations against prosecuting domestic domains reassures all the domestically based websites that expressed concern over SOPA's ability to shut them down. The language of OPEN is clear: OPEN cannot regulate domestic websites. The USITC may not start investigations against domestic domains and must stop any pending investigations under OPEN. Instead, in the event a copyright holder files a complaint against a domestic site, the case is to be referred to the Attorney General for prosecution under domestic copyright law provisions. Domestic copyright law would provide protections for intermediaries, and only lead to the prosecution of willful infringers.

Opposition and Concerns

The creation of OPEN raises several major concerns. The first major issue is the transfer of authority to the USITC.³¹ The USITC is considerably smaller than the Department of Justice (DOJ), with approximately 350 employees compared to over 100,000 in the service of the DOJ. The USITC sets an internal target of 15-16 months for the entire process.³² This sort of time delay in processing could cause irreversible damage to rights holders, as the dissemination of copyrighted material can be expeditious and unstoppable. For example, if a claim of illegal distribution of a top album took 15 months to process, it would essentially be useless given the speed of the music cycle. As a reference, the current record for remaining in the top 100 list is 76 weeks, or about 17 months.³³ Most

²⁹ DesMarais, Christina. *SOPA, PIPA Stalled: Meet the OPEN Act*. PCWorld. http://www.pcworld.com/article/248525/sopa_pipa_stalled_meet_the_open_act.html

³⁰ Fulton, Scott M. *SOPA Opponents Sign On To Wyden-ISSA Alternative Piracy Bill*. Readwrite Enterprise. <http://readwrite.com/2011/12/13/sopa-opponents-sign-on-to-wyde>

³¹ USITC. *About the USITC*. http://www.usitc.gov/press_room/about_usitc.htm

³² "Section 377 Investigations Frequently Asked Questions." United States International Trade Commission, Dec. 2009. Web. 29 Nov. 2012. http://www.usitc.gov/intellectual_property/documents/337_faqs.pdf.

³³ "Section 377 Investigations Frequently Asked Questions." United States International Trade Commission, Dec. 2009. Web. 29 Nov. 2012. http://www.usitc.gov/intellectual_property/documents/337_faqs.pdf

music sales peak within a few weeks of release, so even a judicial victory resulting in injunctive relief would be too little, too late.

Another concern with the USITC is that, as a quasi-judicial organization, it lacks the ultimate authority to stop infringing websites. In reality, if the USITC finds violations of OPEN, it must then refer the case to the DOJ via the Attorney General. This creates a significant level of extra bureaucracy and red tape that could hinder the efforts of law enforcement, and reduce OPEN's effectiveness. Given the speed with which copyright infringers are able to operate, it is crucial to streamline the process as much as possible.

Furthermore, the USITC has a mixed record in dealing with patent disputes. Both the domestic and international communities have raised concerns that the USITC's system is routinely gamed by companies.³⁴ These companies often pursue foreign, domestic and USITC legal action to maximize their chances at favorable outcomes, and it is unclear that the USITC could handle copyright disputes any better.

Opponents of OPEN have also expressed concern for small business and individual artists involving the USITC's involvement. The takedown process requires a significant legal effort on behalf of the companies, which favors large corporations. Small claims would become fiscally impossible or at least impractical while major music labels would definitely benefit from OPEN. The small-time author whose book is being distributed for free online would lack a practical way to seek relief under OPEN.³⁵

Finally, a number of opponents suggest that OPEN will be ineffective at stopping online piracy. Given the ease of migrating domain names with today's technology an infringer could easily move to a new domain name a short time and do so without the knowledge of payment processors or advertisement networks.³⁶ One example of this happening under other laws is the case of FrontRowSports.com. This website, which was dedicated to maintaining streaming links to popular sporting events around the world, was shut down in the United States for broadcast right infringements. However, shortly after the shutdown, a nearly identical website emerged (FrontRowSports.eu) defeating the purpose of the shutdown.

Moreover, *free* distribution cannot be easily stopped with this legislation. As OPEN targets only for-profit websites, free distribution is not within the scope of the act. It is difficult to target free distribution without resorting to some of the proposed methods in SOPA and PIPA. Given the strong opposition to this legislation, it is unlikely that effective legislation targeting free distribution could be passed.

³⁴ Chien, Coleen V. "Patently Protectionist? An Empirical Analysis of Patent Cases at the International Trade Commission." *William & Mary Law Review* 50 (2008): 63-155. Print.

³⁵ The Right Planet. *ICYMI: OPEN Act Emerges as Powerful Alternative to SOPA/PIPA*. Jan 22, 2012. <http://www.therightplanet.com/2012/01/icymi-open-act-emerges-as-powerful-alternative-to-sopapipa/>

³⁶ Smith, Lamar. *OPEN Act Increases Bureaucracy, Won't Stop IP Theft*. <http://judiciary.house.gov/news/01192012.html>

Our Proposal: Modifications to OPEN

Given the aforementioned issues, the following modifications to the existing version of OPEN are proposed:

- Removing USITC Authority and giving it to the DOJ
- More flexible cease and desist orders given to payment processors
- Removal of 1201 Copyright Circumvention clause
- Removing Presidential authority for rejecting USITC findings
- Focus on targeting payment processors primarily through a clearly defined court procedure

Any provision not specifically mentioned in this paper should be left intact. In the next section these provisions will be analyzed for their viability, ability to address existing concerns with OPEN and SOPA, as well as potential implications and opposition. Additionally, an example of a technological solution has been included in Appendix I.

Specific Modifications to the current version of OPEN (H.R. 3782)

Transferring USITC Authority to the DOJ

It is proposed that all instances of “the Commission” (referring to the International Trade Commission) be replaced with the “Department of Justice.”

More flexible cease-and-desist orders to payment processors

This modification to OPEN would allow payment processors to use existing judicial orders to suppress what payment processors determined were simply the same offender using a different alias or domain name.

It is proposed that another paragraph is added between Section 2, subsection (f), paragraph 4 and paragraph 5 which states:

(5) IMMUNITY FOR FURTHER ACTION –

(A) In the instant an Internet site dedicated to infringing activity which has previously received an order issued under this subsection is accessible or has been reconstituted at a different domain name, a financial transaction provider or Internet advertising service may take measures described in subsection (g)(2) with immunity from civil actions except in the case that—

“(i) the site has modified its services to comply with the order previously mentioned.

“(ii) the site has been pardoned of the aforementioned order or the order has expired.

(B) NOTICE.—Upon taking further action, the financial transaction provider or Internet advertising service must provide notice to the

Internet site in question as well as the Department of Justice and the complainant.

(C) REVIEW PERIOD AND COURSE OF ACTION—The Department of Justice will have 7 days from the filing of the notice to determine if the action taken by the financial transaction provider or Internet advertising service in question was just and after must modify and amend the previous order if the action made by the financial transaction provider or Internet advertising service in question is just or

“(i) act pursuant to paragraph C or,

“(ii) in the case that a decision cannot be made, the standard process for filling a temporary or preliminary order will be made.

(C) FALSE REMOVAL OF SERVICE—If an Internet site is found not to be infringing upon the aforementioned order, the financial transaction provider or Internet advertising service in question must immediately undo any restrictions made against the Internet site with respect to the aforementioned order.

(D) REPEATED FALSE ACCUSATIONS—In the case a specific financial transaction provider or Internet advertising service enforces three false removals of service pertaining to the nature of subsection (A) in the course of 90 days, the Department of Justice has the right to prevent the financial transaction provider or Internet advertising service in question further removal of service until a period of 90 days from the date of last prevention.

Removal of the 1201 Copyright Circumvention clause

Currently Section 4, subsection (b) reads:

(b) MERCHANDISE THAT CIRCUMVENTS COPY RIGHTS.

(1) IN GENERAL. Notwithstanding section 1905 of title 18, United States Code, if the Commissioner seizes merchandise that the Commissioner suspects of being imported into the United States in violation of subsection (a)(2) or (b) of section 1201 of title 17, United States Code, the Secretary of Homeland Security may notify a copyright owner described in paragraph (2) of the seizure of the merchandise."

(2) COPYRIGHT OWNER DESCRIBED. A copy right owner described in this paragraph is the owner of a copyright under title 17, United States Code, if merchandise seized on the suspicion of being imported in violation of subsection (a)(2) or (b) of section 1201 of title 17, United States Code

(A) is primarily designed or produced for the purpose of circumventing, has only limited commercially significant purpose or use other than to circumvent, or is marketed for use in

circumventing, a technological measure that effectively controls access to a work protected by that copyright; or
(B) is primarily designed or produced for the purpose of circumventing, has only limited commercially significant purpose or use other than to circumvent, or is marketed for use in circumventing, protection afforded by a technological measure that effectively protects the rights of the copyright owner in a work or a portion of a work.

It is proposed this subsection is struck in its entirety.

More clearly defined court procedure for primarily targeting payment processors

Rights holders are to send notices to financial service providers and the DOJ, following which the internet site in question has 5 days to submit a counterclaim, which gives it temporary immunity from any action that payment processors could take.

It is proposed that the court procedure would work as follows:

1. Complainants must send notices to financial transaction providers or Internet advertising services and the Department of Justice.
2. The Internet Site in question would have 5 business days from the time they are notified to submit an initial counter notice. The website will have the option to file an expedited counter-notice with the Department of Justice following a template provided by the Department of Justice. The template would cover the most common reasons that false-positives are reported, and begin the counterclaim process nearly instantly.
3. After this period one of two things will happen:
 - a. In the case that the Internet Site does not reply with a counter notice, the financial transaction provider or Internet advertising service may take initial action to restrict the Internet Site. Once action has been taken, if a counter notice is filed, then financial transaction provider or Internet advertising service in question must retract their restrictions and the counter claim procedure would continue as if the counter notice was filed initially.
 - b. In the case the counter notice is filed with the Department of Justice, the website will have temporary immunity from action until a decision is made with regards to the complaint.
4. A member of the Department of Justice would then have a week to determine a preliminary course of action.
5. If the Department of Justice makes a preliminary decision to freeze a website's payments the website in question is to be notified of the decision. The Internet site would then have a week to file a more second counter action report disputing the verdict. Any payments that

would be due to the website shall be collected in an escrow account, and held until a final verdict has been reached.

- a. If a second counter notice is filed, then the Department of Justice will have 15 days to make a final decision with an option to extend that time period with difficult cases. Extension requests must be approved by both the Department of Justice and the USITC.
 - i. If the verdict is upheld, the financial transaction providers and Internet advertising services will continue on the same course of action. The payments held in the escrow account are forfeit to the U.S. Treasury Department, net of expenses associated with the escrow account and those incurred by the payment processors in connection with action taken.
 - ii. If the verdict is overturned, all financial services shall be restored within 4 business days, and the contents of the escrow account shall be returned to the website, with interest calculated at the prevailing 5 year treasury rate.
- b. If no second counter notice is filed after a period of one week, the financial transaction provider or Internet advertising service can choose to take action and freeze payments permanently. The payments held in the escrow account are forfeit to the U.S. Treasury Department, net of expenses associated with the escrow account and those incurred by the payment processors in connection with action taken.

Another area of focus for expediting the court procedure is through electronic means. Although is already mentioned in the existing OPEN legislature that the Commission can hold hearings electronically or obtain testimony or other information electronically (Section 2, subsection (e), paragraph (5)) it is proposed that an electronic pre-screening process is established. This should fall under “other information” but it would be beneficial to be explicit about including the pre-appeals process in the legislature.

Solution Analysis

Transferring USITC Authority to the DOJ

By removing the USITC authority provision from OPEN and returning judicial and investigative authority to the Department of Justice, we address several key issues of OPEN's ability to efficiently address infringing websites. The first issue addressed is the ability to process claims quickly. As stated previously, due to its size, the USITC lacks the manpower to process claims as efficiently as a large organization such as the DOJ, where a significant amount of workers are able to put in the time into researching the validity of claims. While OPEN does have a provision that allows the USITC to expedite claims, the bill states that expediting may occur only upon "showing of extraordinary circumstances" (Sec. 2, subsection (f), paragraph 2, subparagraph (E), part (i)) by the claimant. This is a high bar that prevents prompt processing, a key component of protecting the complaining party. Also, this gives priority to larger websites and businesses, hurting small businesses and artists.

It is important to bring up the reasons for which the USITC was initially selected and then discuss why the DOJ would be a better fit. For over 80 years the USITC has been the body through which US rights holders have obtained relief from unfair imports, including ones that violated intellectual property rights. Section 337 of the Tariff Act of 1930 describes how the USITC investigates rights holders' requests for relief.³⁸ Since the agency already employs a transparent process that involves several parties a chance to be heard, the USITC seemed like a good choice.

As previously stated, several parties that opposed SOPA but support OPEN have applauded the selection of the USITC as the agency in charge of enforcement. These organizations believe that this agency can act as a buffer between rights holders and accused infringers. The result of this additional step was supposed to be increased due diligence, and thus a decrease in false positive accusations and shutdowns. For some of the larger websites, a shutdown in operations could be extremely costly. Since the USITC lacked the authority to require a shutdown directly, a website that refuses to comply with a shutdown order can continue to operate normally during the course of the dispute. This mitigates the effect of false positives, and gives importance to the takedown notice and appeals process.

Furthermore, the USITC is a very different type of entity than the DOJ. The USITC's principal role is to act as a dispute mediator, and is focused on bringing two parties together and finding a reasonable course of action. The DOJ is primarily focused on prosecution and the enforcement of U.S. law. The organizations that the DOJ administers include the Drug Enforcement Administration, the Federal Bureau of Investigation and the Federal Bureau of Prisons, among others. It is clear to see that the core mission of the DOJ is bringing criminal elements to justice and ensuring that the law properly processes

³⁸Title 19, Chapter 4-Subtitle II Part II §1337. Unfair Practices in import trade.
<http://www.law.cornell.edu/uscode/text/19/1337>

them. Given that the problem of copyright infringement can potentially affect many parties, it is easy to see why websites and organizations that could be collateral damage or victims of a false positive would be concerned.

The problem with the USITC is that Internet privacy issues and “unfair imports” made through the Internet are extremely different than the imports that Section 337 and the USITC was designed for. Given the incredible speed at which digital “imports” can be distributed, the relevant legal process must also be rapid. The DOJ is a natural candidate for the role of enforcement and processing given its large size and proximity to the American legal system. As mentioned previously, the USITC is a relatively small entity, and is distanced from the enforcement process. We believe that the DOJ is the only entity that is close enough to the process of the law and has the size needed to process requests related to OPEN adequately. Only the DOJ itself can determine if it has any spare capacity to dedicate to copyright enforcement, and a moderate boost in size (~50-100 people) might be in order. Assuming the base DOJ salary of \$62,467, a dedicated copyright task force could reasonably be had for less than \$7 million.³⁹

The same traits that make certain websites and organizations nervous about the selection of the DOJ are reassuring to copyright holders. The solution to dealing with a more powerful and rapid prosecuting body is to make sure that the appeals process is rapid and receives the same amount of attention that the infringement reporting process does.

In the same way that rights holders have a set of tools at their disposal to rapidly identify and propose action against offending websites, the ecosystem of websites that is being affected needs to have equal countermeasures. Having an automated appeals system that allows a website operator to cheaply and quickly challenge any allegations is key. Section 2, subsection (e), paragraph (5) of H.R. 3782 allows for electronic submission of information and proceedings. It allows the Commission, which in our revised proposal would be the DOJ, to hold hearings electronically or obtain testimony or other information electronically at as low a cost as possible to participants. We propose that in addition a pre-appeal screening process using technology such as Skype become standard. This pre-screening could only require non-key judicial personnel, and would serve as a “smell test” to determine which appellees were most likely to be false positives and expedite the appeals process for these people.

A careful analysis of the proposed court procedure shows that at any given moment, a website involved with an infringement claim has the option to file a counter notice. In case a website chooses to file a counter notice, it immediately has immunity from any action that could be taken against it. This means that a website that believes itself to be wrongly targeted can conduct its business as usual during the first stage of the process. Income from advertising networks and transfers carried out by financial institutions will still be valid during the first claim period, and the website can continue operating. Only once an initial investigation of the rights holder’s claim has been conducted will

³⁹ "USDOJ: Legal Careers: Attorney Salaries, Promotions, and Benefits." *USDOJ: Legal Careers: Attorney Salaries, Promotions, and Benefits*. Web. 29 Nov. 2012. <http://www.justice.gov/careers/legal/entry-salary.html>

payments effectively stop to the potential infringing website. Even after an initial verdict has been reached, websites still have a second appeal process open to them, albeit on a longer timeline. Furthermore, any payments that the website would have collected by the website during the course of the process are promptly returned, with interest. Under the proposed system, a website would initially have the benefit of the doubt, as well as the option of an appeal. Furthermore, the whole process is relatively quick, and minimizes financial damage done to innocents. The burden of processing these requests, and the fact that the rights holder needs to file an initial claim should discourage the DOJ from overreaching

Maintaining impartiality is still important, and cutting out the USITC out altogether is unwise. Members of the USITC have institutional knowledge about the processes described in Section 337 and previous enforcement efforts, and could act as consultants to the DOJ. The proposed changes incorporate the USITC as a decision-making body when the DOJ requests an extension on their second processing of a copyright claim. This help make sure that the DOJ does not request extensions that are inappropriate, or designed to “starve out” a website. The USITC is an ideal representative for the interests of the website in question. Websites that feel they have a legitimate counterclaim will be much more likely to contact the USITC and ask for help advocating their case than those that simply decide to run afoul of the law. Furthermore, the USITC can be in charge of maintaining other safeguards that ensure that rights holders do not abuse their right to request a Commission investigation. A rights holder that engages in litigation deemed “excessive” by the DOJ or the USITC may be required to take additional steps before the DOJ is willing to hear their case. Making the USITC the point of contact for complaints from groups opposed to a particular action (such as freedom of speech advocates) could further balance the power distribution.

Removal of §1201 Enforcement – Copyright Circumvention

As currently written, OPEN is meant to protect copyright holders by targeting international, for profit websites whose main business is profiting from illegal distribution of copyrighted works. However, the law also includes a provision on targeting international players based on 17 USC §1201, which prohibits the circumvention of copyright protection methods. While of domestic interest, international copyright circumvention is not an issue that merits equal billing, and has seldom been used to prosecute violations domestically.⁴¹ Given that prosecuting those who break the law internationally is one of the main challenges of OPEN, it seems ambitious to include this provision. If a website’s primary purpose is to distribute and profit from works, the source of the copyrighted material or how protections were circumvented are much less important than the fact that the material is being distributed in the first place. Furthermore, enforcement of this provision is extremely difficult given that copyright circumvention does not directly generate significant advertising or sales revenue. As previously mentioned, targeting the payment sources for infringing websites is the least contentious way to enforce copyright policy. Given that circumvention of a copyright

⁴¹ <https://ojs.lib.byu.edu/spc/index.php/PrelawReview/article/download/13605/13483>

mechanism generates no revenue directly and only becomes profitable when distribution enters the picture, it is clear that the focus needs to remain on distribution.

Attempting to address these two separate but related issues seems like an excellent way to dilute the resources that the bill marshals against online piracy, and distracts from the core mission of the bill. While the DOJ has significant resources, they are not unlimited. Furthermore, §1201 has not proven particularly effective at deterring piracy, and has instead lead to a variety of lawsuits that are anticompetitive in nature and have deterred innocents from innovating.⁴² This piece of legislation has not proven effective and instead has acted as a way for corporate interests to abuse and manipulate the law to establish a competitive position.

Focus on Targeting Payment Processors

While the other proposed modifications are important, targeting payment processors is the most significant in terms of achieving the original purpose of SOPA. By cutting off infringing websites' revenue, the incentive to distribute copyrighted content is severely reduced. Unable to generate revenue, these sites will be forced out of business.

This is a measure that would benefit both the victims and the payment processors. In *Perfect 10 v. Visa*, courts found that payment processors do not have liability for profiting from copyright infringement. Thus, they currently have no legal incentive to target copyright infringers, and have so far been operating on good faith. Payment processors largely comply with government initiatives because they must interact with the government daily in many different ways to curb illegal activities that are facilitated by their networks. This includes very serious offenses such as fraud, money laundering and tax evasion. Furthermore, payment processors do not want to be associated with illegal activities, as it severely damages their reputation and makes it more difficult for them to do business in a market with few points of differentiation. Adding legal incentives and protections would allow the processors to take more responsibility and continue to purge their networks of illegal actors. It would provide additional support for their actions, as current measures are often questionable for them.

One example of a useful legal tool is granting payment processors the ability to pursue multiple online identities under a single infringement notice. Online identities and transaction profiles are easily created and destroyed, and an individual or organization can have several profiles at one time. This brings up an interesting point. What should be done if a user, say "moviestealer100", is receiving payment from a website that infringes on copyright law and gets shut down and then an almost identical user, "moviestealer200", is begins to exhibit the same behavior? In this case, rights holders would be requesting two extremely similar investigations of what is understood to be the same individual. However, the existing language of OPEN would require that the whole process be started once again.

⁴² "Unintended Consequences: Twelve Years under the DMCA | Electronic Frontier Foundation." *Unintended Consequences: Twelve Years under the DMCA | Electronic Frontier Foundation*. 3 Mar. 2010. Web. 08 Nov. 2012. <<https://www.eff.org/wp/unintended-consequences-under-dmca>>.

Payment processors have sophisticated systems that are able to determine various kinds of fraudulent activity based on the profile of the transactions.⁴³ These systems detect patterns of activity and bring notable cases to the attention of administrators. For example, if a credit card is used to buy gasoline and then immediately attempts to make a large jewelry purchase, payment processors know to freeze the account, as this is generally a sign of a stolen card. Once a digital profile of activities has been established for a user, it is possible to track the user across several identities based on patterns of behavior. In agreeing to use a given payment processor's services, users are made to agree to have their data scanned by fraud detection measures such as this. However, payment processors are often hesitant to establish this connection because they do not want the liability of enacting a potential false positive. False positives are harmful to both the business relationships that the processors have, as well as the payment processors' profit margins. By freezing an account on the basis of falsely detecting fraudulent activity, payment processors risk alienating customers who are dependent on regular streams of income to run a legitimate business. Moreover, since processors take a percentage of every transaction, the potential losses from a false shutdown could be harmful to the revenues of both the processor and the company. Given these issues, minimizing false positives is generally of great interest to payment processors, and often a system will flag a suspicious set of transactions and proceed to call or message the customer to confirm whether or not a transaction was fraudulent. Adding this second step in all but the most flagrant instances of fraud has worked well so far with current customers. The proposed legislative changes incorporate this mentality by giving a website the chance to respond and make their case before any action is taken towards them. Only once a website operator has been determined guilty, or upon their failure to respond in a timely manner will any action be taken against them. Although somewhat inconvenient, this additional step should be enough to minimize any damage false positives could cause. Giving the payment processors the freedom to pursue these leads by strengthening their umbrella of protections granted to them would address the problem of speed. When dealing with a stubborn, distributed and fast acting network, it is crucial to have a similarly flexible set of tools at your disposal.

Furthermore, the strong and simplified system of appeals that we have would encourage legitimate operators to complain and halt the process. Illegitimate operators would be much less likely to complain, and by and large would simply ignore the event and move on to a new identity.

In many cases of today, court orders are handed down via *Ex Parte* decisions, cases in which the opposing party does not show up to court. This established system would eliminate the controversy with *Ex Parte* cases and due process. It would require a clear and specific set of guidelines, protections, and limitations, all centered on the current model of DMCA copyright takedown notices expressed on YouTube. It would create a

⁴³ Chen, Brian X. "Some PayPal Users, Frozen Out, Criticize Antifraud Measures." *The New York Times*. The New York Times, 02 Aug. 2012. Web. 08 Nov. 2012. <http://www.nytimes.com/2012/08/02/technology/paypal-antifraud-measures-are-extreme-some-users-say.html?pagewanted=all>.

strong interface for the courts to interact with rights holders and payment processors that allows for the government to provide backing for processors without any worries of liability.

Stakeholder Responses to our Modifications

The proposed solution addresses many of the major concerns with OPEN that were raised earlier by its opponents. Beginning with the transfer of authority from the USITC back to the DOJ, those who were concerned that the USITC lacked the capacity to enforce OPEN will be happy with the proposed changes. One agency that will likely respond positively to this change is The Motion Picture Association of America (MPAA), which strongly opposed the initial draft of OPEN because it took too long to prosecute infringing sites.⁴⁴ Moving the process back to the DOJ will likely expedite prosecution. Overall however, it is expected that the MPAA will not be entirely supportive of the proposed bill because the bill still does not address search engines. Another group mentioned by the MPAA that will likely respond positively, small businesses and artists, are better represented with the new judicial process proposed.

It is also predicted supporters of OPEN (mentioned on KeepTheWebOpen⁴⁵) will remain in support of our new proposed bill. Two of the changes that might create contention is moving authority to the DOJ from the USITC and giving financial transaction providers and Internet advertising services the ability to act on doppelgangers. The first of these will likely not detract supporters because the process through which Internet sites are tried is extremely similar to the bill in the original legislature, it is just being performed by a body that is more well suited to do so. The second might be a little more controversial because financial transaction providers and Internet advertising services have the ability to act on their own but important safeguards were put in place to prevent these groups from acting potentially infringing Internet Sites without strong evidence. However, the fact that steps have been taken to ensure a robust appeals process should serve to partially mitigate these concerns. Most importantly, the legislation will not affect parties until they have been found initially guilty by an American court of law. The “innocent until proven guilty” approach is a cornerstone of the American legal system, and should keep any concerns from seriously affecting the coalition.

⁴⁴ <http://blog.mpaa.org/BlogOS/post/2012/01/30/OPEN-Act-Falls-Short-.aspx>

⁴⁵ <http://www.keepthewebopen.com/supporters>

Evaluation of Proposed Solution

When deciding how to address the copyright option, there are several options. One option is to do nothing, and let the Internet continue to operate as it does. A second is to attempt to revive SOPA/PIPA. A third is to accept OPEN as it is, and make no modifications to it. We believe each option is more compelling than the preceding one, but none are as compelling as the fourth option proposed in this paper: a modified version of OPEN.

A Course of Inaction

The first, and most simple approach is simply to do nothing. All the legislation that is proposed contemplates establishing a separate zone based on the geographic limits of the United States. This concept is flawed, as there is no easy way to differentiate digital goods based on their origin or establish barriers on the Internet that mirror political borders. Doing nothing also eliminates the problem of false positives. With any action-based solution, the lack of perfect information can lead to false positives. It is also possible that any legislation would drive payment processors and advertising networks abroad, or at least severely burden them with legislation that is present nowhere else in the world. Even legitimate websites might shift their operations overseas because they wanted to reduce the risk of being targeted. Furthermore, whether any real financial damage is being done to the copyright holders has yet to be concretely established. For example, while the MPAA estimates copyright infringement costs the movie industry \$20.5 billion a year, other sources came up with a figure of only \$446 million using the same data.⁴⁶ The actual cost is difficult to pin down, as there are many different ways to count the cost and it is not clear that one is “more right” than another.

However, it is unacceptable to say merely because a problem is difficult, it is not worth pursuing. The United States is increasingly transitioning to a service and knowledge based economy, and it will be important to provide the regulatory tools for giving these industries a fair shot. The film, game and music industries in particular are industries that have traditionally been very strong in the United States, and have been able to remain relevant and important over time. The United States has a unique opportunity to establish a precedent that will set the framework for the rest of the world’s copyright protection efforts and should proceed accordingly.

Reviving past legislation

A second alternative to explore is reviving PIPA/SOPA. These two pieces of legislation have a different approach to the same problem that OPEN and modified OPEN address. During a recent panel at the 2012 Consumer Electronic Show (CEW), the executive director of the Copyright Alliance Sandra Aistars made the case for SOPA.⁴⁸ She explained that the current iteration of SOPA had fixed problems with the bill and had

⁴⁶ http://www.washingtonpost.com/blogs/wonkblog/post/how-much-does-online-piracy-really-cost-the-economy/2012/01/05/gIQAXknNdP_blog.html

⁴⁸ Brodtkin, Jon. "ArsTechnica." *Ars Technica*. N.p., 10 Jan. 2012. Web. 07 Nov. 2012. <<http://arstechnica.com/tech-policy/2012/01/fighting-internet-piracy-ces-takes-on-sopa-vs-open-debate/>>.

narrowed its scope, targeting only websites that were designed to distribute complete copies of protected material for financial gain.

One of the principal objections detractors of SOPA raise is that it is overbroad, would target sites like Facebook or Reddit, and would impose technology mandates on site operators. Unlike SOPA, OPEN creates a much more expensive process that would be inaccessible as a legal remedy to smaller copyright holders. Including the USITC would add a layer of complication that simply is not there in SOPA. Furthermore, SOPA targets a variety of fraudulent websites, including those that distribute illegal physical goods such as imitation prescription drugs.

However, the underlying issues with SOPA and PIPA remain. It is concerning that current language makes it possible for legitimate websites to be targeted and forced to shut down. It has been shown that a nontrivial percentage of DMCA takedown notices are fraudulent, and untangling the associated legal issues has proven especially difficult for small businesses. Major corporations such as Universal Music have been accused of using the DMCA system to gain a negotiating advantage, a clear abuse of the system.⁴⁹ Adding in SOPA and PIPA to the mix will only boost the number of false positives. Furthermore, the approach taken by these bills is drastic, and it is plausible that legitimate websites that accidentally host copyrighted content can be targeted. An excellent example would be online chatrooms and forums. SOPA and PIPA create a framework for Internet censorship –once implemented it could expand in scope and be used to clamp down on a variety of activities, not just copyright infringement.

On a practical note, both SOPA and PIPA are stalled out in the House of Representatives and Senate, respectively. Opposition from a variety of influential groups has made these bills incredibly contentious. Even if it were possible to amend them in such a way that made sense, SOPA and PIPA are still politically toxic, and are unlikely to pass soon, if ever.

OPEN is a much more targeted response, and addresses only the group of infringing websites that are outside the United States. In and of itself, this removes a huge amount of the opposition that was encountered with SOPA and PIPA, and makes the bill much more politically feasible. Furthermore, as previously stated, OPEN has several structural improvements over SOPA and PIPA that are extremely important and attractive. First of all, the actions that OPEN generates in response to a copyright allegation have a more transparent appeals process, and help protect from false positives. This number of false positives should be significantly lower than under SOPA and PIPA to begin with (thanks to the reduced scope) and should make the law much more manageable and easier to implement. In particular, OPEN only targets foreign websites that are conducting business in the US, and whose core operation is the willful infringement of copyrighted works. The definition and scope is sufficiently tailored to avoid many missteps.

⁴⁹ <http://boingboing.net/2011/07/20/universal-music-accu.html>

The tools available to OPEN are more limited as well, and the legislation stays away from the extremely contentious DNS targeting issues. These two raised many objections from Internet experts and freedom of speech advocates. Instead, the legislation focuses on voluntary collaboration of existing payment and advertisement processors.

Modified OPEN

Despite major improvements over SOPA and PIPA, there are several weaknesses that OPEN fails to address. As previously stated, the bill has a provision for enforcing copyright circumvention violations. The whole point of reducing the scope of the bill was to ensure that the bill was narrowly targeted and addressed a very specific set of requirements. Modified OPEN refocuses the legislation on websites that distribute copyrighted material abroad, and makes sure to remain narrowly tailored.

OPEN also errs by being too cautious. Giving authority to the USITC instead of the DOJ and not taking advantage of an opportunity to include increased protections for payment processors underutilizes the opportunity that the legislation presents. The modifications that have been proposed to OPEN return to the DOJ, and give the legislation real teeth. Simultaneously, the modifications to OPEN are designed to minimize the damage that could be inflicted by false positives on legitimate website operators. The process is essentially a two step process that gives website operators the benefit of the doubt and the ability to contest charges as easily as rights holders can present them, if not more easily. Furthermore, the USITC remains somewhat involved to act as a third party and deter judicial overreach. The proposed modifications to OPEN also give payment processors the ability to pursue infringers that are operating under aliases or are attempting to repeat behavior, something that is impossible under the current language of OPEN.

Conclusion

As discussed in this document, the U.S. currently faces a problem with enforcing copyright abroad. Lack of jurisdiction and a dearth of cooperative governments mean that a significant amount of websites distribute copyrighted material for profit. Previous attempts at legislation proved controversial, and failed to pass. The second generation of legislative efforts resulted in OPEN, which addressed many of the problems that groups had with SOPA and PIPA. This paper discussed OPEN, and the need for several modifications to the existing language of the legislation to achieve maximum effectiveness. The changes breakdown to three points: returning authority to the DOJ and strengthening the legal protections afforded to payment processors, removing distracting pieces of side legislation, and turning focus to target payment processors through a defined court procedure.

Many steps are needed to push the modified version of OPEN through the U.S. legislative system, beginning with the generation of support for these changes. Industry-sponsored groups whose sole purpose is to educate government officials and the public on the positive outcomes of these changes would be extremely useful for raising awareness of the modified bill. As shown by PIPA and SOPA, certain key actors such as Google and Wikipedia wield enormous power. Contacting representatives and senators with a track record of similar viewpoints will prove useful as well. Once there are legitimate backers of the modified version of OPEN, the next step is to approach the USITC and the DOJ. Both organizations play an important role in the proposed enforcement process, and it will be useful to get feedback from key officials in these organizations. Helping officials understand their role under the modified legislation, and getting feedback on the feasibility of their proposed responsibilities will lead a more tailored piece of legislation. The language included in this document is preliminary at best, and may raise objections from powerful interest groups that have not been addressed in this document.

Another step in the process is gathering ideas and gauging the feasibility of any technological tools that can be designed to assist with enforcement. Since any technical solution would deal with complicated analysis algorithms and have hardware requirements, a cost-benefit analysis must be performed to determine what levels of each maximize efficiency. Third-party software specialists are an excellent starting point, since many of these problems already have commercial solutions. As a starting point, an example proposal has been included as appendix I of this document. The proposal is based on the existing national copyright registry..

It is clear that there must be a greater legal infrastructure to combat the problem of online piracy and illegal media distribution. The policy changes proposed in this document are a starting point, and are based on legislation that is currently being debated. The modified version of OPED does not address every problem associated with illegal distribution of copyrighted material, but is a start. By implementing the above modifications to OPEN and combining that with new technology, the United States can lead the transition to a safer and more efficient world for copyrighted material.

Appendix I: Example Technological Solution

Recommended Technological Approach

Even with the proposed modifications to OPEN, a key problem still remains with the distribution of media on the Internet. It is not always clear what material is copyrighted and what is not, and the question ultimately changes into with what is being distributed both legally and illegally. On a national scale, measures can be put into place to maintain information on copyrighted content and legal distributors of this content. The problem of illegal media distribution is an international one though, and it is becoming necessary for a global database of copyright information. Only then can we make headway on this global problem.

Current Approach

Copyright information is currently stored and maintained by the United States Copyright Office, which is part of the Library of Congress. Due to changes made by the Copyright Act of 1976, a person in the United States who authors a work will automatically get protection under a copyright on that creation. It is not required for the author to register the work with the Copyright Office, but it is possible for an author to do so. By filling out an application either online or through the mail, the author can register the copyright in the Library of Congress' system. The author must also mail a copy of the work directly to the office in order for the copyright to be approved. The author of a work must register in order to proceed with a copyright infringement action, and that is where the benefit of registering lies.⁵⁰

This current system however is not perfect, and there is a loophole to get around this registration step. The copyrightability of a work can be considered in court before addressing the issue of infringement, so it is still possible to file these infringement lawsuits without being in the copyright system. The interface to register is also extremely outdated and can take longer than what is necessary for such a simple step. The current online system recommends IE6 or Netscape Navigator, and the process of sending the work via the mail system is not time or cost efficient. All works can and should be updated electronically. Ultimately, there should exist greater incentive for the author to register in the copyright system, and the process should be easier. The system should also have the capability to connect with similar systems in participating nations. The following technological approach solves these problems.

Global Copyright Database

The purpose of this database is to establish a central location with information that can be used to expedite the detection and prosecution steps of finding and processing copyright violators. This database is also useful to internal and external (non-US jurisdiction) enforcement efforts. Eventually, this database could be used as a reference point for more automated copyright infringement detection systems, but it will currently be used to

⁵⁰ <http://law.lexisnexis.com/infopro/zimmermans/disp.aspx?z=1342>

determine where rights belong. Although the United States Copyright Office currently controls the copyright database, the Department of Justice (DOJ) should have advanced querying abilities and the power to request additional information from authors and rights holders.

The database should initially be broken into two main information areas: a collection of information pertaining to the identification of all relevant copyrighted material and a collection of legal media distributors for each piece of copyrighted material in the first collection. There are two steps to this process, and it involves gathering data on current material that exists and adding data as new media is copyrighted. Because the initial creation of a database containing all copyrighted material and legal distributors is a technological hardship, the information should be garbage collected frequently to prevent the exponential growth in server space and processing power requirements. There will have to be requirements placed on those who own the copyright to ensure accuracy in the database, and will be aided by a quick application process. This infrastructure allows flexibility to manage and connect data that flows into it, but it is necessary for the owners of copyrighted material to cooperate in order for the infrastructure to be successful.

The first step is to create a database of all relevant copyrighted material. There are three main players in the creation of this system: the Copyright Office service center controlling the database, the actual authors and rights holders, and the distributors of media content. A diagram of the flow of information can be seen in Figure 1 on the following page. These groups must work together in order for this database to be successful, and an example of tasks for each group can be seen in the relevant arrows.

The Library of Congress, specifically the Copyright Office, will be the authoritative source of data pertaining to copyright information in the United States, but they will rely on information from other sources of data. These sources will hopefully be the original owners of these media rights (publishers, writers, and CRMs). In order to make this process as seamless as possible, a user system should be created that allows holders of rights to register with the system and then transfer the necessary information without the need of a middleman. This system currently exists in a basic form, but the application process needs to be made simpler. There must also be technical infrastructure in place to determine and solve conflicts of the entering of data, and each user can be monitored on the quality of their submission. This data integrity will be ensured through a small application process that requires minimal human analysis.

Rights holders must pass any relevant information pertaining to their media content to the service center. The Copyright Office can then take that information and enter it into the database. This constant updating of information ensures that copyright information is up to date, but it does not ensure that the data is comprehensive across the world. Only then will this database be powerful. In order to maintain a high participation in this information reporting process, policy should be put in place to require this transfer of data to the Copyright Office. The current policy contains loopholes. Reporting copyright information should be made a prerequisite to being able to file copyright lawsuits. Rights holders have no incentive to withhold their information, and would make this step a part

of their business cycle. These steps handle the updating of future copyrighted material that emerges, but gaining information on past material is still a technological issue. The source of this information must again be the holders of rights and the current database maintained by the Copyright Office. If a rights holder believes that their past work is still capable of losing money through illegal distribution via the Internet, it is his responsibility to pass this copyright information to the DOJ. A case study should be written on the subject; it is certain that copyrighted material has a certain window of profit-generating capability, but how long is this window typically open for different types of media?

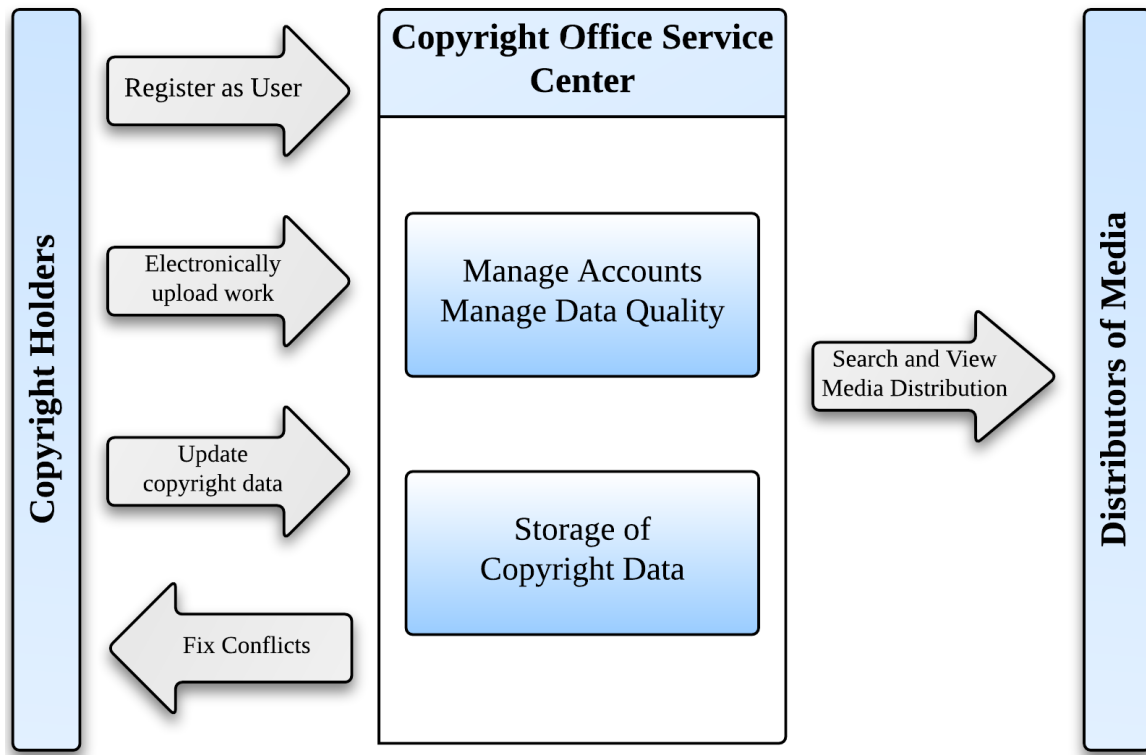


Figure 1. Representation of the central Copyright Office Service Center and role of the holders of copyright and media distributors

The second step in the creation of this global database pertains to the storage of information relating to the legal distributors of pieces of copyrighted information. This database currently does not exist in any way, and the Copyright Office must create the infrastructure to collect and maintain this data. Fortunately the process and structure is similar to the database for copyright registration. The data stored here is closer in granularity to the discussed problem of identifying distribution channels. As mentioned with the storage of copyrighted material information, it is in the hands of the rights holders to provide the Copyright Office with this information. This step is a much more involved process and will require more effort on the rights holders side; information is constantly being added, deleted, and modified for specific pieces of copyrighted material. This problem calls for a simple query and insertion system that can be used by rights holders to update distributor information real-time. A simple representation of this

process is seen in Figure 2. Again, policy should be created to make it a requirement for holders of these copyrights to create and maintain their entries in this system. This policy should be less stringent since legal distributors are created every day, but it must ensure that the authors and rights holders are compliant with any queries by the Copyright Office or the DOJ. The original technological problem concerns the free distribution of copyrighted material. Knowing who can legally distribute media and who can't gives the DOJ a huge advantage in determining which distributors are acting illegally, and it also provides infrastructure to determine who is distributing under fair use.

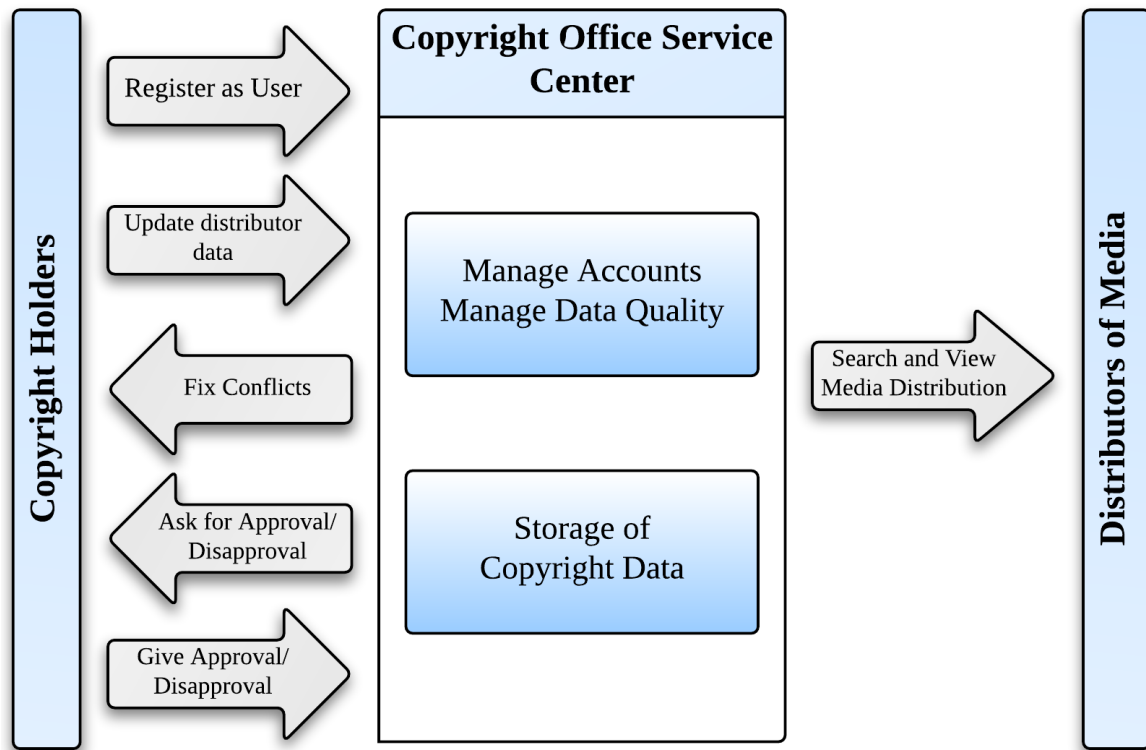


Figure 2. Representation of the central Copyright Office Service Center and the storage of data pertaining to the distributors of copyright information. A similar user system is used as explained in Figure 2.

Imagine the scenario where a music publisher releases a song to be distributed (sold) across the Internet. The publisher will register as a user with the Copyright Office Global Copyright Database and will then have the ability to update the system with relevant copyright information pertaining to the song. The next step for the publisher is to determine and relay information relating to the legal distributors of this song on the internet. An example of a legal distributor would be iTunes, Amazon, or another third-party application that allows the downloading of a song. The DOJ would then have the responsibility of querying distributors of the above mentioned song; if a distributor exists that is not currently in the Global Copyright Database, then the DOJ must go back to the publisher (either through the Copyright Office or straight through to the publisher) and relay this information. The publisher must then approve the distribution or disapprove the distribution. If the media is approved, the Copyright Office creates a new entry into the database that contains the information relating to that distributor and the specific piece of

copyright information. It may also be the case that this distributor now also has the approval to distribute other songs by the same publisher; if this is the case, then the Copyright Office now has the responsibility to update the legal distributors database accordingly for the new piece(s) of media. If the media is disapproved for distribution by this medium, the legalities of this distribution must be analyzed on an individual basis. If in fact the media was deemed distributed illegally, the DOJ can take the appropriate measures of enforcing the law. If the distribution was done internationally, the DOJ can contact the relevant nation that has a similar infrastructure in place. The DOJ can also be contacted by other nations regarding the illegal distribution in the United States of international media. It is clear that the Copyright Office and the DOJ must have infrastructure in place to communicate effectively.

The amount of data being stored in these databases will be extremely large and will grow exponentially in the future. It is therefore imperative to design a protocol for garbage collecting, throwing out data that is no longer relevant for our purposes. There should be two metrics for measuring how relevant a piece of copyright information currently is in our database: how often it is flagged as being something that is distributed illegally and how long it has been since its initial release. Knowing these two pieces of information, a system can be created to routinely inspect the database and determine which entries can be deleted so as to trim the fat in the system. If a piece of media content is not consistently being distributed illegally or it has not recently been distributed illegally, it does not make sense for it to take up space in our database, as the focus of the database is to aid enforcement and detection efforts. This information can be obtained from our data analysis algorithms mentioned previously. Also, the further from the date of creation, the less a piece of copyright material is able to generate revenue for those who own the rights. From this premise, we can use this time information to determine if an older work no longer has financial reason to be contained in our database. The obvious extreme is works that are about to pass into the public domain and no longer generate revenues. This garbage-collecting step is necessary to reduce server storage costs and processing power requirements and must therefore not be taken lightly.

The Global Copyright Database should be housed within the Copyright Office where its predecessor currently stands. The analysts must also be members of the copyright office. The actual technological design however can be contracted out, and requirements should be issued and put-out for bids among private developers. The team needed to maintain such a database and monitor the distribution of media will need to be on the order of 100 employees. Deloitte, with the ICE Global Repertoire Database, required 75 employees to manage a database of 16 million copyrighted data records.⁵¹ While there will be significantly more data records when different pieces of media are included in the database (music, movies, books, etc.), the use of existing data platforms can help the Copyright Office make the work more efficient. This technological approach would also create the need for more analysts, therefore creating jobs in the Information Technology sector, a key position in a struggling economy.

⁵¹ <http://globalrepertoiredatabase.com/rfir/ICE%20GRD%20RFI%20Response.pdf>

Role of the Department of Justice

The Copyright Office clearly controls the database and its entries, but the examination of illegal distributors of media will come from the DOJ. The DOJ must then have the necessary measures in place to have the ability to contact authors/rights holders and submit information to the Copyright Office. The current querying system will be sufficient for the public, but a more advanced system should be available to the DOJ in order to find any information they need on the rights holders. It does not make sense to house the system in the DOJ since the current system exists in the Copyright Office within the Library of Congress. For this implementation to actually come into existence, the current system must be altered while passing certain jobs onto the DOJ.

Next Steps

This approach can be implemented from a national standpoint due to the infrastructure that currently exists in the United States Copyright Office; the most complex portion of this proposal involves international policy, and it is necessary that other governments jump on board for this project to be successful. It must be made clear to other nations that Internet piracy is a problem, and there is only upside in the implementation of this technological approach. Another barrier is the opponents of the original OPEN legislation. It should be transparently stressed that this approach does not involve the over watch of "Big Brother," and all information stored in these databases is legally sourced from the rights holders via some degree of connection. The biggest problem will be the funding for the project, however media publishers could very well be a proponent of a tax if it means they will save money in the long-run. A case-study be done on this subject as well, because self-funded ventures are much more likely to get passed.

The Global Copyright Database provides nations with the ability to originate and maintain copyright records for media copyrighted in their nation. It also gives them the ability to maintain a fairly comprehensive set of information pertaining to the legal distributors of data. The quality of this data can be checked with the originator of the copyright information and is therefore accurate enough for the use of this infrastructure. With this information in hand, the DOJ has the ability to monitor media distribution on the Internet and enforce United States' law if applicable. Nations also have the ability to help each other out which is necessary to solve this global problem. This technological recommendation is however just a proposal for the above amendments to OPEN, and it should be taken as so when submitted to Congress; technology created the problem of Internet piracy, but technology can also be our ally in the fight against illegal media distribution.

Appendix II: A Brief History of Peer-to-Peer Piracy

Prior to the expansion of the dot-com bubble in the late 1990's, online piracy was of relatively little significance and not well known. Speeds were much too slow to allow for any meaningful transfer of media using the Internet, and piracy was not a concern. However, as the Internet grew faster and larger several tools that enabled piracy emerged. Among these were the Peer-to-Peer (P2P) software tools and websites, most notably Napster in 1999. Napster allowed the transfer of files by maintaining a centralized database of user-file possession relations and facilitating the direct download of requested files between a searching client and possessing client.⁵² The system was robust and easy to use, and an example of how a system like Napster would work is given in Figure 3.

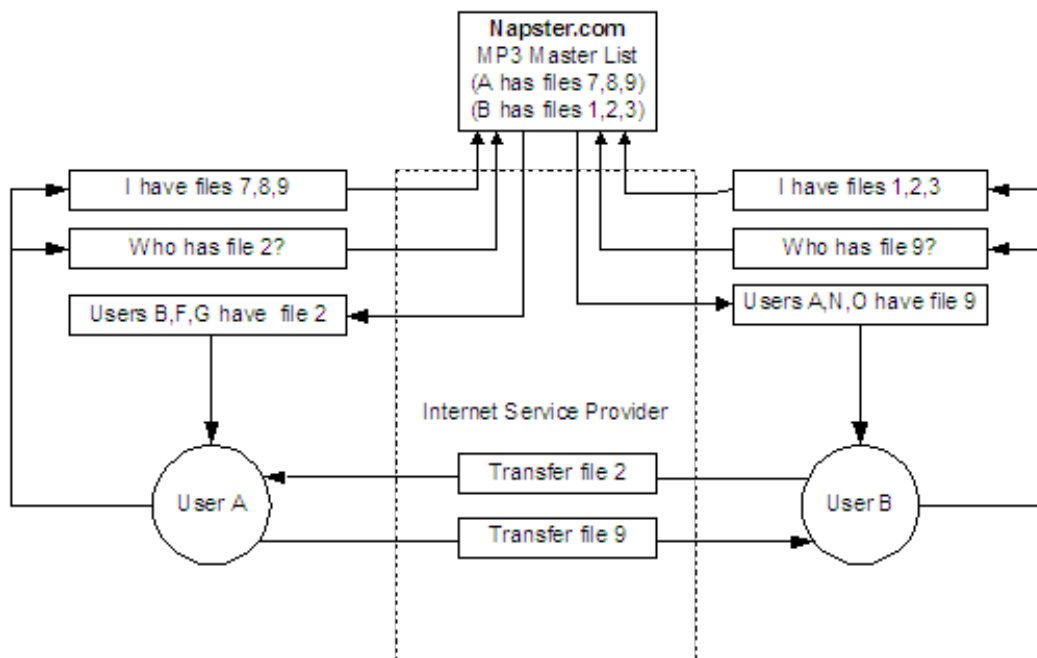


Figure 3. Sample Peer-to-peer network scenario.

However, following the shutdown of Napster's P2P service in July 2001 as a contributory and vicarious infringer,⁵³ a number of prominent other P2P services emerged, including LimeWire and Kazaa.

While Kazaa was essentially a copy of Napster developed by a competitor, LimeWire used the Gnutella protocol as part of the so-called second generation of P2P software. The Gnutella protocol attempted to fortify the P2P services against shutdown with the use of a decentralized system that required the shutdown of all of its servers, or *nodes* to stop the service. Unlike the centralized system of the first generation, the Gnutella protocol has clients broadcast requests to all available nodes, which then relay it to other nodes

⁵² Douglas, Guy. *Copyright and Peer-to-Peer File Sharing: The Argument Against Legislative Reform*. Murdoch University Electronic Journal of Law. (March 2004)

⁵³ Pfaffenberger, Bryan. *The Napster Decision: What is it all about?*. Linux Journal. Feb 13 2001

until the requested file can be found and downloaded⁵⁴. Limewire, Kazaa, and others were all either shut down or forced into a pay-only membership system to settle lawsuits from the RIAA.⁵⁵ This led to the development of the third, and current generation of P2P networks, known as BitTorrent.

⁵⁴ Stanford University CS244b. *The Gnutella Protocol Specification v0.4*.
http://www.stanford.edu/class/cs244b/gnutella_protocol_0.4.pdf

⁵⁵ Purewall, Sarah Jacobssen. *Limewire Shuts Down Permanently*. PC World, Oct. 27 2010.
http://www.pcworld.com/article/208895/Limewire_Shut_Down_Permanently.html

Bibliography

"Unintended Consequences: Twelve Years under the DMCA | Electronic Frontier Foundation." *Unintended Consequences: Twelve Years under the DMCA | Electronic Frontier Foundation*. 3 Mar. 2010. Web. 08 Nov. 2012.

<https://www.eff.org/wp/unintended-consequences-under-dmca>.

Bittorrent.org. *The BitTorrent Protocol Specification*.

http://www.bittorrent.org/beps/bep_0003.html

Brodkin, Jon. "ArsTechnica." *Ars Technica*. N.p., 10 Jan. 2012. Web. 07 Nov. 2012.

<http://arstechnica.com/tech-policy/2012/01/fighting-internet-piracy-ces-takes-on-sopa-vs-open-debate/>

Center for Democracy and Technology. *Intermediary Liability: Protecting Internet Platforms For Expression and Innovation*. April 2010.

[https://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_\(2010\).pdf](https://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf)

Center for Democracy and Technology. *Intermediary Liability: Protecting Internet Platforms For Expression and Innovation*. April 2010.

[https://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_\(2010\).pdf](https://www.cdt.org/files/pdfs/CDT-Intermediary%20Liability_(2010).pdf)

Chen, Brian X. "Some PayPal Users, Frozen Out, Criticize Antifraud Measures." *The New York Times*. The New York Times, 02 Aug. 2012. Web. 08 Nov. 2012.

<http://www.nytimes.com/2012/08/02/technology/paypal-antifraud-measures-are-extreme-some-users-say.html?pagewanted=all>.

Chien, Coleen V. "Patently Protectionist? An Empirical Analysis of Patent Cases at the International Trade Commission." *William & Mary Law Review* 50 (2008): 63-155. Print.

Definitions, United States Copyright Office. <http://www.copyright.gov/help/faq/faq-definitions.html>

DesMarais, Christina. *SOPA, PIPA Stalled: Meet the OPEN Act*. PCWorld.

http://www.pcworld.com/article/248525/sopa_pipa_stalled_meet_the_open_act.html

Douglas, Guy. *Copyright and Peer-to-Peer File Sharing: The Argument Against Legislative Reform*. Murdoch University Electronic Journal of Law. (March 2004)

Fahrenthold, David A. *SOPA Protests Shut Down Websites*. Washington Post.

http://www.washingtonpost.com/politics/sopa-protests-to-shut-down-websites/2012/01/17/gIQA4WYl6P_story.html

Fahrenthold, David A. *SOPA Protests Shut Down Websites*. Washington Post.

http://www.washingtonpost.com/politics/sopa-protests-to-shut-down-websites/2012/01/17/gIQA4WYl6P_story.html

Fulton, Scott M. *SOPA Opponents Sign On To Wyden-ISSA Alternative Piracy Bill*. Readwrite Enterprise. <http://readwrite.com/2011/12/13/sopa-opponents-sign-on-to-wyde>¹ USITC. *About the USITC*. http://www.usitc.gov/press_room/about_usitc.html

House Judiciary Committee. *Stop Online Piracy Summary*. October 26, 2011. <http://judiciary.house.gov/issues/Rouge%20Websites/Stop%20Online%20Piracy%20Summary.pdf>

House Judiciary Committee. *Stop Online Piracy Summary*. October 26, 2011. <http://judiciary.house.gov/issues/Rouge%20Websites/Stop%20Online%20Piracy%20Summary.pdf>

HR 3261. *The Stop Online Piracy Act*. <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3261>
Pepitone, Julianne. *SOPA Explained*. http://money.cnn.com/2012/01/17/technology/sopa_explained/index.html

Pepitone, Julianne. *SOPA Explained*. http://money.cnn.com/2012/01/17/technology/sopa_explained/index.html

Pfaffenberger, Bryan. *The Napster Decision: What is it all about?*. Linux Journal. Feb 13 2001

Purewall, Sarah Jacobssen. *Limewire Shuts Down Permanently*. PC World, Oct. 27 2010. http://www.pcworld.com/article/208895/Limewire_Shut_Down_Permanently.html

Singer, Bill. “Bah Humbug! ‘Operation In Our Sites’ Nabs 150 Websites On Cyber-Monday.” *Forbes*, November 28, 2011, sec. Investing. <http://www.forbes.com/sites/%20billsinger/2011/11/28/bah-humbug-operation-in-our-sites-nabs-150-websites-on-cyber-monday/>

Smith, Lamar. *OPEN Act Increases Bureaucracy, Won’t Stop IP Theft*. <http://judiciary.house.gov/news/01192012.html>

Stanford University CS244b. *The Gnutella Protocol Specification v0.4*. http://www.stanford.edu/class/cs244b/gnutella_protocol_0.4.pdf

The Right Planet. *ICYMI: OPEN Act Emerges as Powerful Alternative to SOPA/PIPA*. Jan 22, 2012. <http://www.therightplanet.com/2012/01/icymi-open-act-emerges-as-powerful-alternative-to-sopapipa/>

Title 19, Chapter 4-Subtitle II Part II §1337. Unfair Practices in import trade. <http://www.law.cornell.edu/uscode/text/19/1337>

United States Constitution. National Archives. http://www.archives.gov/exhibits/charters/constitution_transcript.html